



Global Fraud Report

Economist Intelligence
Unit survey results

Sector by sector analyses
of fraud

Regional fraud insights

The use of technology in
helping & hindering fraud

Regulatory updates

Global & local case studies

And many more articles

Kroll commissioned The Economist Intelligence Unit to conduct a worldwide survey on fraud and its effect on business during 2009. A total of 729 senior executives took part in this survey. A little over a third of the respondents were based in North and South America, 25% in Asia-Pacific, just over a quarter in Europe and 11% in the Middle East and Africa.

Ten industries were covered, with no fewer than 50 respondents drawn from each industry. The highest number of respondents came from the financial services industry (12%). A total of 46% of the companies polled had global annual revenues in excess of \$1billion.

This report brings together these survey results with the experience and expertise of Kroll and a selection of its affiliates. It includes content written by The Economist Intelligence Unit and other third parties.

Kroll would like to thank The Economist Intelligence Unit, Dr. Paul Kielstra and all the authors for their contributions in producing this report.

The information contained herein is based on sources and analysis we believe reliable and should be understood to be general management information only. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such. Statements concerning financial, regulatory or legal matters should be understood to be general observations based solely on our experience as risk consultants and may not be relied upon as financial, regulatory or legal advice, which we are not authorized to provide. All such matters should be reviewed with appropriately qualified advisors in these areas.

This document is owned by Kroll and The Economist Intelligence Unit Ltd., and its contents, or any portion thereof, may not be copied or reproduced in any form without the permission of Kroll. Clients may distribute for their own internal purposes only.

Kroll is a subsidiary of Marsh & McLennan Companies, Inc (NYSE:MMC), the global professional services firm.

Global Fraud Report

INTRODUCTION	4	HEALTHCARE, PHARMACEUTICALS & BIOTECHNOLOGY	
Tim Whipple, President, Kroll Consulting Services		A glimpse into Mexico's shadow pharmaceutical market ...	24
EIU OVERVIEW	5	TECHNOLOGY, MEDIA & TELECOMS	
The Economist Intelligence Unit overview		IT outsourcing: Is it worth the risk?.....	26
FRAUD VULNERABILITY		NATURAL RESOURCES	
Summary of sector fraud profiles.....	8	The Foreign Corrupt Practices Act, the Siemens settlement, and the energy sector	27
REGIONAL ANALYSIS		REGIONAL ANALYSIS	
Asia-Pacific overview.....	9	Middle East & Africa overview.....	29
FINANCIAL SERVICES		RETAIL, WHOLESALE & DISTRIBUTION	
Fighting credit card fraud:		India's retail sector:	
Don't overlook the low-tech battle	10	Risks that match the potential rewards	30
But how could they do that to us?:		VIEWPOINT	
The growth of affinity frauds	11	Multiple-source reporting: What works for tax fraud could work for Ponzi schemes	32
When the law lets you down.....	12	CONSUMER GOODS	
Buyer beware: Information security and M&A activity.....	13	Chinese fakes in Korean markets.....	34
Financial crime: What should insurers be worrying about?	14	TRAVEL, LEISURE & TRANSPORTATION	
PROFESSIONAL SERVICES		Fraud risks in commercial aviation.....	36
The pitfalls of arbitration.....	15	CONSTRUCTION	
Tackling client and data problems	16	Three predictions for the future: The impact of the global economy on construction	38
REGIONAL ANALYSIS		FRAUD VULNERABILITY	
North America overview	18	Fraud heatmap: where industry feels the pain, and how it reacts	40
Europe overview.....	19	Slowdown in business expansion drives reduction in fraud factors	42
MANUFACTURING		Corruption fears grow.....	42
Tackling compliance with conviction.....	20	KROLL CONTACTS	43
VIEWPOINT			
The United Kingdom's new anti-bribery legislation	22		
Not all identity theft is high-tech, and no one is immune.....	23		

Introduction



We all hope that the worst of the financial crisis is behind us – and most of us do not want to look back. This has been a year of painful adjustment in the harsh conditions of recession. The prospects for 2010 look brighter, leaving us less inclined to focus on the mistakes that brought us to this pass.

Yet there is ample reason to cast a glance over our shoulders as we look forward to the happier tasks of the new recovery. Fraud, corruption, and all that go with it may not have precipitated recession, but they certainly made its impact all the more painful. Losses, prosecutions, litigation, bankruptcies, were all sparked or exacerbated by the actions of groups or individuals in the years before; actions that went undetected and unpunished until too late.

The conventional wisdom is that fraud goes up in a recession. That isn't necessarily true, as our survey shows. What goes up is the discovery of fraud, not always the same thing. Just like legitimate businesses, fraudsters are threatened by loss of income or the financial weakness of their businesses; Ponzi schemes are especially vulnerable. But other fraudulent areas – management conflict of interest, corruption, employee theft – also come to light when business conditions sour.

The data we have collected this year clearly highlights the industry hardest hit by fraud and wrongdoing: financial services. Over half of the respondents in this sector reported that the global financial crisis had increased levels of fraud at their companies – the highest figure for any industry. Nearly 90 percent of firms reported being victims of some kind of fraud in the last three years. This sector also had the second highest proportion suffering from each of internal financial fraud and management self-dealing.

Unfortunately, though, over one in five financial services companies saw their internal controls weakened through cost cutting. It is understandable that in today's climate, they should seek economies. But these will be false economies over the longer term if they lead to the resurgence of the same issues that so deeply damaged the industry in 2008-9.

“Tighter controls” will not be a popular rallying cry in Wall Street, the City or Nariman Point. The associated costs can be hard to bear in difficult times – but the cost of non-compliance can be harsher. Compliance professionals know they have to provide value for money. In the risk management world, so do we. That means investment in people, systems, training and capabilities, to make sure that as the world's leading global firm in the sector, Kroll can provide the best support. We have continued to invest throughout the recession, and next year will bring new ideas to the market. This report sets out some of the reasons why those ideas have never been more important.

TIM WHIPPLE
President, Kroll Consulting Services

Economist Intelligence Unit overview

The downturn and fraud

Your sector may even be better off

The conventional wisdom – reinforced by the revelation in the last year of huge scams such as the Madoff and Satyam frauds – is that downturns increase levels of fraud. This year's annual Global Fraud Survey, commissioned by Kroll and carried out by the Economist Intelligence Unit, presents a much more complex picture. The financial crisis has changed the effects of the risks underlying fraud. Those risks that grow as companies expand – entry into new markets, for example – have actually declined in importance. In simple terms, less money coming into a company and more oversight of spending despite financial constraints limit the opportunity for crime.

The downturn, however, has heightened other risks. Pay stringency in the face of lower revenues, for example, has provided a motive for fraud, and perhaps even turned employees to crime. How these conflicting trends play out, however, varies markedly by sector. Those closer to the original crisis – financial services and professional services in particular – have seen an increase in their incidence and level of fraud. Those for whom the main economic news has been a pronounced drop in sales, and therefore business activity – such as construction and natural resources – have instead seen noticeable declines. Economy-wide the two trends cancel each other out to a remarkable degree. The incidence of fraud is almost identical to that found in last year's survey, and the average loss per company has risen only slightly in the new survey, to \$8.8 million from \$8.2 million.



From which of the following has your company suffered in the last three years?

	2009 survey	2008 survey
At least one fraud	85%	86%
Theft of physical assets or stock	38%	37%
Information theft, loss or attack	25%	27%
Management conflict of interest	23%	26%
Financial mismanagement	21%	22%
Regulatory or compliance breach	21%	25%
Vendor, supplier or procurement fraud	20%	18%
Corruption and bribery	19%	20%
Internal financial fraud or theft	18%	19%
IP theft, piracy or counterfeiting	14%	16%
Money laundering	5%	4%

The downturn has increased the motive for fraud, but decreased the opportunity.

The economic crisis in isolation has raised some fraud risks. Thirty percent of survey respondents say that the global financial crisis has increased the levels of fraud at their organizations, compared with just 5 percent who saw a decline. Lower profits heighten some risks. One in six companies are seeing greater vulnerability from reducing internal controls to save money, one in seven from pay restraint, and one in eight from reduced revenues overall.

A constrained business environment, however, reduces other dangers as businesses and individuals adopt more defensive behavior. Survival-focused companies might retrench rather than expand; employees might stay in existing jobs rather than take a chance on new ones. As a result, three factors which often increase fraud vulnerability are having noticeably less effect this year. The number reporting that high staff turnover is raising such exposure has dropped (from 32 percent to 26 percent), as has the number seeing greater risk out of entry into new markets (from 32 percent to 24 percent) and from increased inter-firm collaboration (from 28 percent to 20 percent). Moreover, if companies take in less money in sales, they also have less money to steal. Companies would rarely cut down on business activity simply to reduce fraud, but at least there is a silver lining.

A Tale of Two Sectors: Changing risks have had vastly different impacts in different industries.

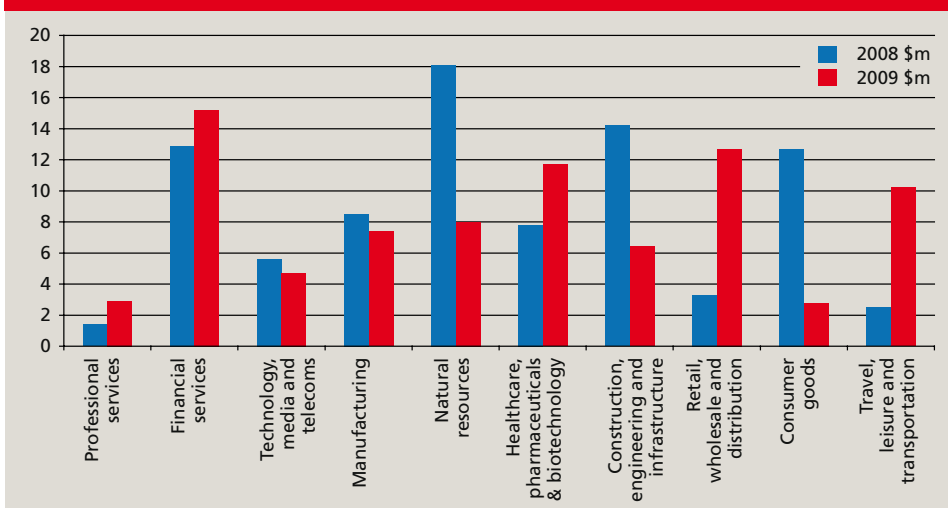
The contrasting fortunes of the financial services and construction sectors illustrate how these shifts have had such different effects. The former, the epicenter of the financial crisis, saw combined average losses to fraud over the last three years rise to \$15.2 million, or 18 percent above the 2008 survey figure. The number of sector companies suffering at least one fraud rose to 87 percent, slightly above the survey norm, from 79 percent, comfortably below. Most notably, over one-half of respondents indicated that the crisis had led to an increase in the number of cases of fraud at their companies.

The picture for the construction, engineering and infrastructure industry is markedly different. In this sector, the combined average fraud figure dropped by more than one-half, to \$6.4 million from

Percentage of companies highly or moderately vulnerable

	2009 survey	2008 survey
Information theft, loss or attack	71%	65%
Regulatory or compliance breach	54%	50%
Management conflict of interest	53%	48%
Financial mismanagement	52%	48%
Vendor, supplier or procurement fraud	51%	54%
Theft of physical assets or stock	50%	53%
IP theft, piracy or counterfeiting	47%	44%
Corruption and bribery	44%	47%
Internal financial fraud or theft	44%	45%
Money laundering	19%	19%

Industry sector/average amount lost to fraud in previous 3 years





\$14.2 million, making the sector's losses, for once, below the average level. The demands of survival in a downturn are also having an impact on which types of fraud are more prevalent for these companies. At a time when government contracts are of increasing importance, and may even mean the difference between survival and collapse, corruption and bribery have seen a marked increase from the levels reported in 2008. Conversely, with much less money to steal, management conflict of interest is down noticeably and, with fewer projects, even compliance breaches have declined.

These types of changes, albeit on a less dramatic scale, have occurred across the economy. Professional services, for example, another sector close to the financial crisis, has seen a marked increase in fraud. Meanwhile, natural resources companies, which have also suffered in the last twelve months from a decline in revenues, have seen a drop in fraud levels. Whether the downturn brings more fraud depends on the line of work.

At the economy-wide level, the contrasting tendencies have almost cancelled each other out.

A variety of data indicate that the net change in the fraud picture is tiny, and may even be zero.

■ **Most see only a slight change at company level:** As noted earlier, respondents believed that the financial crisis itself had increased levels of fraud. When asked, however, about the last year – precisely when the downturn has been taking its toll – in more general terms, 31 percent said that fraud levels had declined, and an additional 34 percent had experienced no change. Only 21 percent had noted a rise. More importantly, any shift was muted: 67 percent saw a slight change, at most, in either direction; only 22 percent reported a substantial change.

■ **Overall, the incidence of fraud and related levels of worry in this year's survey are almost identical to those of last year:** Suffering some kind of fraud is the overwhelming norm in business, but this has long been the case. The table on page 6 gives the percentage of the firms hit by the various categories of frauds in the last three years according to the current survey as well as the corresponding figures from the 2008 survey. The relative ordering has changed little, and all but two of this year's numbers are within 2 percent of those from the previous survey – the kind of differences that could easily appear in two surveys taken at the same time.

Similarly, the percentage of respondents who considered their companies highly or moderately vulnerable to these frauds stayed roughly the same as last year, albeit with slightly greater variation.

■ **The average fraud loss has risen slightly in the last year, but this masks larger, countervailing changes across the economy:** The average combined loss to fraud per surveyed company for the last three years was \$8.8 million, only 7 percent higher than the 2008 survey figure of \$8.2 million. This hides greater underlying change. Five of the sectors covered in this report saw increases in their average losses, and five saw declines. Moreover, while in this year's survey larger companies – those with over \$5 billion in annual sales – reported greater average losses, up to \$25.8 million from \$23.3 million in the 2008 survey, the situation actually improved for smaller business – those with yearly revenues under \$5 billion – dropping to \$4.6 million from \$5.5 million.

The change is likely to last only as long as the downturn.

Although in the aggregate, fraud levels are little changed, this reflects a substantial shift in business behaviour, which is increasing certain types of fraud risks and diminishing others. Much of this is driven by the downturn, which has left some sectors far more exposed to fraud than others. Just as the current economic situation is temporary, however, these shifts are likely to reverse with renewed growth. Companies should beware, that when volumes and profits start to rise, the fraud risk kaleidoscope will take another turn.



Summary of sector fraud profiles

Sector	Exposure (degree to which sector is exposed to fraud)	Response (degree to which sector has adopted fraud countermeasures)	Comment
Financial services	HIGH	HIGH	Financial services has the broadest exposure to fraud issues: money laundering, financial mismanagement, regulatory and compliance, internal financial fraud and information loss or theft. It faces the most severe threat of any sector from money laundering and regulatory or compliance breaches. Its exposure in other words, is both deep and broad. It also has the highest adoption of anti-fraud measures: it focuses on financial controls, staff background checking, reputation management, risk officers and risk management systems.
Professional services	LOW	LOW	Professional services has the most narrowly focused set of fraud issues: only information theft, loss or attack is a serious hazard. Its levels of investment in fraud management are similarly low compared to other sectors.
Manufacturing	HIGH	HIGH	Manufacturing's issues are significant, and primarily internal and staff-related: theft of assets and stock, financial mismanagement, and IP theft, as well as (in some cases) bribery and corruption. The sector has invested in due diligences on partners, vendors and clients; staff training and whistleblower hotlines; IP protection; and physical security.
Healthcare, pharmaceuticals and biotechnology	MODERATE	MODERATE	This sector has a narrower set of challenges than some others: financial mismanagement, regulatory and compliance, and IP theft, piracy and counterfeiting. Compared with other sectors, it has invested significantly in IP protection and staff screening.
Technology, media and telecoms	LOW	LOW	TMT has a narrow set of issues around information – IP theft and information loss or theft (to which it is the most vulnerable). The sector has a greater focus than others on IT security.
Natural resources	MODERATE	HIGH	Natural resources confronts bribery and corruption, theft of assets, and management conflict of interest. Its patterns of operations raise its risk profile. The sector (which has received a lot of criticism) has invested in due diligences on partners, clients and vendors; staff training; reputation management; and risk management systems.
Retail, wholesale and distribution	HIGH	LOW	Predictably, this sector's biggest issue is with theft of stock; it also has a persistent set of issues around internal financial fraud or theft and vendor fraud. All of these result directly from its operations and structure – reliance on large groups of suppliers, often geographically very widely set apart. The addition of information loss or theft indicates the trend towards regarding information as a highly valuable asset that is vulnerable. But its investment in fraud countermeasures is generally lower than in other sectors with the exception of asset protection and physical security systems, reflecting its focus on loss prevention as the primary approach.
Consumer goods	MODERATE	MODERATE	Consumer goods companies have a relatively narrow set of issues to face: theft of assets and stock, vendor, supplier and procurement fraud, and IP theft, piracy and counterfeiting. But they face the most serious threats of any sector in the first two categories, caused by their extended supply chains. It has strongly adopted financial controls, IP protection measures and physical asset protection.
Travel, leisure and transportation	MODERATE	MODERATE	This diverse sector faces issues with theft of assets, management conflict of interest and (especially) internal financial fraud. Very often, the businesses present complex financial flows and are vulnerable to manipulation. It focuses fraud countermeasures around staff screening, reflecting its role as a people business.
Construction, engineering and infrastructure	HIGH	MODERATE	Construction, engineering and infrastructure companies face particular concerns with corruption and bribery, financial mismanagement, regulatory and compliance breaches, and vendor, supplier and procurement fraud. It is an example of an industry with widespread fraud issues caused by its risk profile – its supply chain, but also the nature of its contracts and operations. It invests in a broad range of fraud countermeasures – but at only average levels, for the most part.

ASIA-PACIFIC OVERVIEW

In the Asia-Pacific region, as elsewhere in the world, the downturn has impeded the ability of fraudsters to operate even as it has done the same for legitimate business.

- The average loss per company over the last three years fell noticeably from the 2008 figure, from \$9.1 million to \$6.2 million. With less money coming in, there is less money to steal.
- Although the number of companies experiencing theft of physical assets in the last three years (43%) increased slightly from the 2008 figure (41%) and was the highest for any region, every other category of fraud saw less prevalence – albeit often not much – than in the previous survey. Overall, the number of respondents suffering from at least one fraud in the last three years dipped just slightly, from 88% in the 2008 survey to 84% this time.
- Only 22% of those surveyed saw an increase in the prevalence of fraud at their companies, against 37% who experienced a decline.

The survey suggests, however, that employee relationships continue to present a challenge across the region, and that corruption may grow as an issue.

- High staff turnover is again this year the most common factor increasing the vulnerability of Asia-Pacific companies to fraud, cited by 35% of respondents. This is the second highest of the five regional figures on staff turnover, and well above the overall average of 26%.
- Although reduced revenue on its own increased fraud exposure at only 10% of firms, the stringency around pay and remuneration which accompanied the downturn raised vulnerability to 18%, also the second highest figure.
- Even while the number of companies which experienced corruption or bribery fell slightly in this survey from the last, from 21% to 17%, the proportion considering themselves highly vulnerable rose to 15% from 10%. The large amount of stimulus spending across the region may account for this greater concern.

On the ground, Kroll is seeing a substantial number of fraud cases, not just current ones but those that began much earlier – the Satyam fraud, for example, had been going on for years before the downturn made it impossible to hide. With the big emerging economies of China and India apparently starting to leave behind the effects of the global economic crisis, the small respite which the downturn gave to fraud incidence is likely to be short-lived.



Spotlight on China

Fraud remains the Achilles heel of Chinese economic development and it goes beyond poor IP protection. In the latest survey, 96% of companies said that they had experienced at least one type of fraud in the last three years. Particular areas of concern are: vendor or procurement fraud (42% have suffered in the last three years, compared to just 21% for the whole Asia-Pacific region), internal financial fraud (31% to 18%), regulatory breaches (31% to 21%), corruption and bribery (27% to 17%), and of course IP theft (23% to 13%). In all of these cases, the regional figures are not very far off the global ones.

	2009	2008
Financial Loss: Average loss per company over last three years	\$6.2 million (71% of average)	\$9.1 million (111% of average)
Prevalence: Companies suffering fraud loss over last three years	84%	88%
High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable	Information theft, loss or attack (22%) Corruption and bribery (15%)	Information theft, loss or attack (27%) IP theft, piracy or counterfeiting (17%)
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in last three years	Theft of physical assets or stock (43%) Information theft, loss or attack (26%) Vendor, supplier or procurement fraud (21%) Regulatory or compliance breach (21%)	Theft of physical assets or stock (41%) Information theft, loss or attack (31%) Regulatory or compliance breach (28%) Management conflict of interest (28%) Financial mismanagement (23%) Vendor, supplier or procurement fraud (22%) Corruption and bribery (21%) Internal financial fraud or theft (21%)

Fighting credit card fraud: Don't overlook the low-tech battle



John Price

In August this year, an extraordinary case of identity theft and credit card fraud came to light in the United States, involving 130 million credit and debit card numbers stolen between 2006 and 2008. According to government investigators, the culprits, including 28-year old master hacker Albert Gonzalez, infiltrated the computer networks of Heartland Payment systems – a leading credit card payment processor – and several major retailers. The prominent case focused attention on the increasingly complex cyber war between criminals and the credit card industry, and will likely spur new firewalls, state-of-the-art software solutions, and well-trained IT security consultancies.

Although such a response is necessary – the fastest growing forms of card fraud are of the high-tech kind – mature market banks and their IT security apparatus are winning this war. In percentage terms, credit card theft rates in the United States and Europe have steadily declined over the last decade. Banks in emerging markets, however,

continue to lose their battle with credit card fraud, particularly of an old fashioned, mundane, yet ultimately more costly type.

In 2007, card fraud globally took in an estimated \$5.5 billion, a startling number, but just 0.05 percent of the total card transaction volume, two percent of what card companies charge for their services, and even less than what issuers earn in interest from customers.

While card fraud losses are a mere pin prick for United States card issuers, losses in emerging markets are far more substantial. In Brazil in 2008, according to Kroll's analysis, this fraud reached an estimated \$300 million, or 0.15 percent of the transaction volume – three times the global average. In Colombia, where banks are arguably less sophisticated than Brazil, losses approach 0.25 percent of total card volume or eight times the United States average.

In July, this year's annual Latin American Tarjetas y Medios de Pago (Cards and Payments Systems) conference attracted leaders from the region's burgeoning card industry. At a Kroll-led workshop, about 50 participants recounted their most recent fraud "war stories".

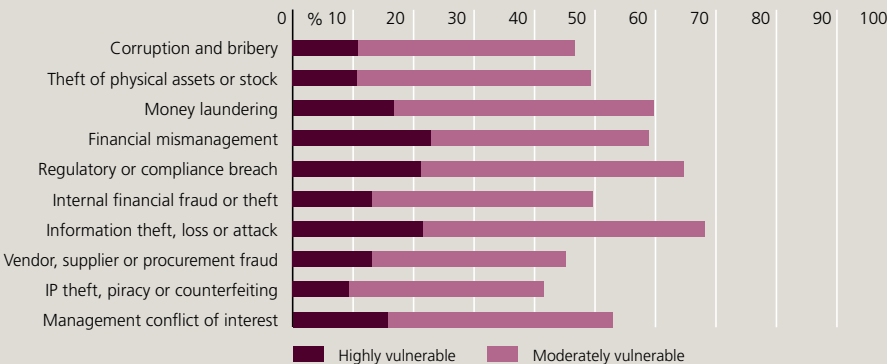
One Brazilian bank's outsourced ATM maintenance supplier had inserted data stripping devices to copy PIN numbers and other bank data from cards used in the machines. A retailer in Colombia recounted how corrupt employees had, in collaboration with criminal elements, installed devices at the register to copy data from cards swiped there and sell it for the production of cloned cards. One Caribbean bank – a leading issuer – explained how members of its own IT department had downloaded card holder identities from its own computers. A Mexican bank described how its ATMs were being ripped out of walls by forklifts, after which the computers inside the machines were hacked and the numbers stolen.

What these stories highlight was that most of the fraud was committed by employees or vendors. Moreover, all the guilty parties had some criminal record that had not been discovered in the internal background-checking process of hiring or contracting. In the case of the "smash and grab" forklift theft, the surveillance equipment and systems were not functioning, victims of budget cuts. The most galling conclusion reached by seminar participants was how preventable most of these episodes were.

While the "arms race" between hackers and IT security may involve strategies incomprehensible to most card industry decision makers, issuers and processors can prevent the majority of frauds by following disciplined protocols in areas such as third-party administered background checks, due diligence on key vendors, the handling of sensitive data, and third-party audited IT security. Furthermore, a regular, external vetting of operations for vulnerabilities will help root out the largely internal sources of fraud. High-tech defenses alone cannot beat low-tech crime.

REPORT CARD FINANCIAL SERVICES

Financial Loss: Average loss per company over past three years \$15.2 million (173% of average)
Prevalence: Companies suffering fraud loss over past three years 87%
Increase in Exposure: Companies where exposure to fraud has increased 86%
High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable to specific frauds
 Regulatory or compliance breach (25%) • Financial mismanagement (23%) • Information theft, loss or attack (22%)
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in last three years
 Theft of physical assets or stock (31%) • Internal financial fraud or theft (29%) • Management conflict of interest (26%) • Information theft, loss or attack (24%) • Financial mismanagement (23%) • Regulatory or compliance breach (21%)
Investment Focus: Percentage of firms investing in this type of fraud prevention in the next year: IT security (63%)
 Financial controls (57%) • Management controls (50%) • Staff training (38%) • Risk management systems (38%)
 Physical asset security (37%) • Staff screening (37%) • Due diligence (36%) • Reputation monitoring (36%)



John Price is a managing director for Business Intelligence in Latin America. He has led business intelligence cases since 1992, when he moved to Mexico City for seven years. As a co-author of *Can Latin America Compete?*, and as a frequently published author on regional business risk and opportunity issues, John is a recognized business intelligence thought leader in Latin America.

But how could they do that to us?:

The growth of affinity frauds

Peter Turecek

Whether due to increased investor skepticism, regulators' need to demonstrate active enforcement, the financial media's search for good copy, an increase in fraud in the current economy, or a combination of all of the above, investment frauds have been coming to light more and more frequently.

The scams, most of them classic Ponzi schemes, involve investment in diverse vehicles, including securities, hedge funds, real estate, investment clubs, and so on. Many, though, have one thing in common: the victims share some trait with the perpetrators of the fraud. This element in common with the fraudster lulls the victims and makes them more readily trusting of the con artist's pitch. The perpetrator preys upon that inherent trust of a shared bond. After all, the fraudster is "one of us" and must be "looking out for me." These are called "affinity frauds."

In the past year, multiple scams have targeted specifically identifiable groups of victims. Targets have included those who are geographically connected, such as high net worth individuals resident in New York City or Palm Beach; investors from certain religious faiths, such as the Jewish or Mormon communities; members of ethnic groups, such as Haitian-, Chinese-, or Korean-Americans; and even the elderly or those with disabilities. Affinity fraud can be based on almost any common bond: victims in the past have come from groups of pilots, former professional football players, divorcees, and members of specific-interest clubs.

In August of this year, the Securities and Exchange Commission (SEC) moved against at least three alleged investment frauds targeting specific communities of victims:

- a man was charged with fraud after he raised over \$1 million from parishioners of a Redding, California church community in a Ponzi scheme;
- a complaint was filed against a Pomona, California-based individual running an investment fraud aimed at mobile home park community residents;

- an enforcement action was initiated against an Orlando, Florida-based individual running a pyramid scheme aimed initially at Orlando and Puerto Rico-based investors.

Even where fraudsters do not share a common trait with their victims, they work to co-opt influential members of the target group. These leaders are typically duped into believing in the investment opportunity, which then spreads by word of mouth to the rest of the community: "If the pastor believes in this opportunity, who am I to disagree?"

Fortunately, most of these situations can be avoided relatively easily. All that is required is a combination of a little common sense and due diligence.

If an investment opportunity promises returns that sound too good to be true – such as incredibly high rates of return or overly consistent returns despite volatile market conditions – it most likely IS too good to be true;

If the investment opportunity cannot be explained to you in a way that readily makes sense, be suspicious. Keep asking questions until you feel comfortable that you understand the opportunity fully.

If the opportunity is a "secret" one, with very limited participation, run the other way;

- Check with your state securities regulator, the Financial Industry Regulatory Authority, or the SEC to see whether the person offering the investment is registered or has a disciplinary history;
- Listen to your instincts. You would be surprised how accurate that little voice can be.



Peter Turecek is a senior managing director in the New York office. He is an authority in due diligence, multinational investigations, and hedge fund related business intelligence services. He also conducts a variety of other investigations related to asset searches, corporate contests, employee integrity, securities fraud, business intelligence, and crisis management. He has appeared on MSNBC, CNBC, Fox News, and NPR and has served as a guest speaker on a number of topics for various investment and professional groups.

EIU SURVEY

A bad year: It has been an annus horribilis for the financial services industry in many ways, and fraud is no exception.

- The average loss per company over the last three years rose to \$15.2 million, 173% of the survey average, and roughly one-sixth more than the 2008 survey figure (\$12.9 million).
- Over one-half of respondents (51%) reported that the global financial crisis had increased levels of fraud at their companies – the highest figure for any sector. Moreover, 35% said that they had seen an increase in fraud in general in the last year, compared with just 28% who saw a decline. This made the sector one of only two where the former outweighed the latter, and it did so by the biggest margin.
- 87% of firms reported being victims of some kind of fraud in the last three years, up from 79% in the previous survey.
- Finally, the sector had the second-highest proportion suffering from each of internal financial fraud (29%) and management conflict of interest (26%), as well as the highest rate of money laundering (10%).

Efforts to address the problem: The industry realizes it has a problem, and is devoting resources to it, but not always consistently.

- For every type of fraud covered in the survey, the proportion of companies considering themselves highly vulnerable increased from last year. Moreover, the industry has the highest proportion of highly vulnerable companies for four out of ten types of fraud – regulatory or compliance breach (25%), financial mismanagement (23%), money laundering (17%) and management conflict of interest (16%).
- Only 2% of financial services firms are not making anti-fraud investments in the coming year, and for nine out of the ten anti-fraud strategies listed in the survey, over one-third of respondents are boosting defenses – the most widespread spending of any sector. In four specific areas, investment will be more common in this sector than anywhere else: IT security (63%), management controls (50%), risk management systems (38%) and reputation monitoring (36%). The first of these is particularly important, as complex IT infrastructures are increasing fraud vulnerability at 46% of sector firms, the highest rate for any industry.
- Unfortunately, however, over one in five companies (21%) saw their internal controls weakened as a result of cost cutting – a tie for the second-worst record of any sector.

As part of their rebuilding in the wake of the recent turmoil, financial services companies need to toughen their anti-fraud defenses. Many are doing so vigorously, but the best controls in the world will fail if, in any future crisis, they are sacrificed to save money.

Written by The Economist Intelligence Unit

When the law lets you down



Commercial solutions for bad investments in Southeast Asia

Chris Leahy

For hedge fund, private equity, and other financial investors in Southeast Asia's emerging markets, restructuring soured deals may seem straightforward enough given the tight legal arrangements usually wrapped around such investments. What happens, though, when the counterparty to the deal, typically the controlling shareholder or sponsor of the company behind the investment, does not cooperate? Similarly, of what practical use is the Singapore legal structure – often adopted in such deals – if the underlying assets lie in a less legally-robust jurisdiction? In certain Southeast Asian markets, questionable judicial independence and a poor track record of upholding the rights of foreign investors mean domestic sponsors often play dirty to retain control of their assets.

It is possible for hedge funds and private equity investors to formulate commercial solutions for exit and recovery when they fall victim to fraudulent or suspect action from sponsors and other counterparties in what, for a foreign investor, can become de facto non-enforceable legal jurisdictions.

The process begins once investors are convinced that legal remedies alone are unlikely, at the very least, to produce an acceptable outcome. The first step is to help them identify the commercial imperatives that will drive the exit and recovery strategy. Key to any approach is the collation of relevant, actionable commercial intelligence in-country. This feeds into an

assessment of the financial position of the sponsors; their objectives, motivation, and anticipated strategy with respect to the dispute and any potential, resultant litigation; the views and assessments of other investors and creditors; and their likely appetite for a negotiated settlement.

This research taps into information from a variety of sources, including customers and suppliers of the company, banks, other financiers, investors, and management. In such inquiries, the objectives should be: first, to gain a better understanding of the practical commercial position of the investor with respect to recovery and, if possible, to improve it; second, to compile a list of viable options and alternatives for the investor; and third, to provide an action plan with the aim of exiting the investment in a commercially acceptable way including, if possible, viable recovery options.

Kroll recently advised a client with an investment that had soured in a Thai manufacturer. The sponsor of the company had grown ever more uncooperative in attempted negotiations, and the investor became suspicious of certain trading patterns within the company. The latter were suggestive of attempts to siphon off money from what was clearly an increasingly distressed business. After a complex investigation that entailed intensive source inquiries, we were able to gather intelligence and evidence that supported the investor's suspicions and to assist in formulating an appropriate commercial strategy to exit the investment.

Kroll was also called in by a hedge fund seeking assistance with a complex debt restructuring for an Indonesian conglomerate that had run into financial trouble. The sponsor's treatment of creditors, coupled with suspicious trading patterns of the growing debt of the group, suggested that the sponsor, through a friendly private equity fund, was perhaps attempting to retain control of his companies. He was doing this by engineering a debt restructuring that would severely disadvantage, and possibly even defraud, existing creditors. We identified the complicit fund and gathered intelligence that supported the client's theory, strengthening considerably its commercial leverage in negotiating a successful conclusion to the restructuring.

As these two examples show, legal remedies are not the only ones which can help when investments go sour. A detailed knowledge of the positions and motives of all parties can lead to strategies which are effective, even where the law might be of little practical help.



Chris Leahy is a managing director in the Singapore office with a particular focus on the financial services industry. This follows a successful 23 year career as an investment banker, CFO, consultant and journalist. Chris began his career in the UK as a stockbroker before joining Peregrine/BNP Paribas and later Crosby, based in Hong Kong, where he was managing director with responsibility for the firm's regional investment banking business.

Buyer beware: Information security and M&A activity

Stephen D. Baird

A key goal in Mergers and Acquisitions (M&A) is to create economic value greater than the sum of the two companies separately. One of the transaction risks often overlooked is the information security footprint of the organizations involved. With data security threats at an all time high, and with imperiled companies forced to make painful and risky cuts in their information security budgets, the prudent corporate suitor should insist on a thorough information security assessment as part of routine due diligence. Using a company's own information security team and an outside expert can significantly reduce related cyber risks.

Many companies evaluating strategic transactions consider the potential costs and benefits of integrating workforces, facilities, functions, and IT systems. The compatibility of information security postures, however, is often left out. A significant gap between the information security approaches of the two companies can result in substantial unanticipated costs. Assessing compatibility in this field is not a simple task: very little uniformity in approach exists beyond the basics of firewalls and virus protection. For example, many companies still have not implemented full-disk encryption for corporate laptops. Many others have not deployed robust intrusion detection or prevention systems, let alone maintained sufficient qualified staff to monitor and maintain them. Facing increasingly sophisticated attacks – both internal and external – on their corporate intellectual property, credit card numbers, and other identity data, even a company with state-of-the-art defenses a year ago may be dangerously under protected today. Two companies that are adequately

protected as standalone entities might expose themselves to risk during integration if their approaches to information security are incompatible.

An internal or external expert can help the M&A team to make informed decisions by providing a security assessment, helping to evaluate the target company's security program, integrating the two security organizations, and assessing the potential impact of information security risks on competitiveness, financial loss, and legal liability.

An information security due diligence investigation assesses a range of risks including: intellectual property loss; flaws in incident response methodology or information asset identification; security gaps created by absorbing and integrating unknown and differing technologies post-transaction; employee technology usage discrepancies; data leakage; and insider malfeasance.

Beyond due diligence, information security expertise can assist with every phase of the M&A process. Leakage of information relating to the deal – anything from unsecured e-mail transmission to loss of printed documents – can cause significant damage or even jeopardize the transaction. Consequently, all relevant staff should be made aware of the gravity of non-compliance with basic security rules. In fact, companies should consider adopting special secure communication measures for all personnel involved in evaluating a potential deal.

If the risks surrounding information security are ignored, a potentially profitable merger or acquisition may fail to deliver anticipated returns, and the organization may have to incur significant costs along with a loss of goodwill, reputation, and possibly future business opportunities.

Points to Consider

1. A seasoned and well-rounded M&A team should include internal or external information security experts. Depending on the nature of the merger and perceived level of risk, these experts can be advisory or proactive.
2. An IT security audit and vulnerability assessment as part of M&A due diligence can assure management that the acquired organization follows best practices in this area. If not readily available, request copies of any external audit or assessment findings and work with the acquisition's legal department to understand the laws, regulations, and standards with which it must comply.
3. An information security monitoring protocol instituted for all phases of the acquisition process will help ensure the confidentiality and integrity of the process and its associated communications.
4. Identifying key information assets and their locations through a risk assessment process is necessary to understand what you are trying to protect, and hence its value to the acquirer. Accurate information asset definitions will assist in the selection of controls to defend that data. The overarching goal is to protect organizational information assets, contribute to the security of interdependent critical infrastructures, and thus help protect the company's intellectual property.
5. Ensure that your security team establishes metrics to measure progress on the complete assimilation of information technology and information security management programs. These should provide information about the state of completion of risk assessments, security impact analyses, and information security plans for all critical systems and business entities after consolidation.
6. Review all contracts and third-party relationships. Any third party security monitoring should in particular be reviewed to ensure that no lapses of important security logging, review, and oversight occur during the M&A process.



Stephen Baird is managing director for Kroll Ontrack's Information Security, Computer Forensics, and ESI Consulting group. He has over 20 years of industry and law enforcement expertise in complex technology and risk mitigation leadership.

Financial crime: What should insurers be worrying about?

Brendan Hawthorne

With governments and regulators worldwide handing out ever increasing fines for data security breaches, bribery, corruption, money laundering, and market abuse, insurance companies are finding it increasingly difficult to know on which financial crime risks to focus their limited resources.

In terms of pure monetary loss, they should begin with claims fraud. This problem is estimated to cost general insurance companies up to seven percent of gross written premium. Other estimates put the amount undetected in the United Kingdom at over US\$3 billion each year. Flourishing organized gangs orchestrate induced vehicle accidents, as well as bogus arson, disability, and healthcare claims. These groups often include doctors and lawyers who support their frauds.

Policyholder fraud in the life insurance industry, on the other hand, tends to revolve around fraudulent surrenders. The extent is difficult to quantify because of the long-term nature of the business and infrequent contact with policyholders. By the time a real policyholder comes forward to claim funds, the fraudsters are often long gone. Organized gangs target call centers or government offices to elicit personal information to enable them fraudulently to surrender policies. Another common tactic is to get gang members employment in insurance companies in order to determine which policies have shown very little activity in recent years: by targeting these, fraudsters can remain undetected for long periods.

Insurance companies also cannot afford to ignore employee fraud. Although its monetary cost is usually less than that of claims fraud, these cases often attract extensive negative media and regulatory interest. Increasingly, organized crime groups place people in companies with a

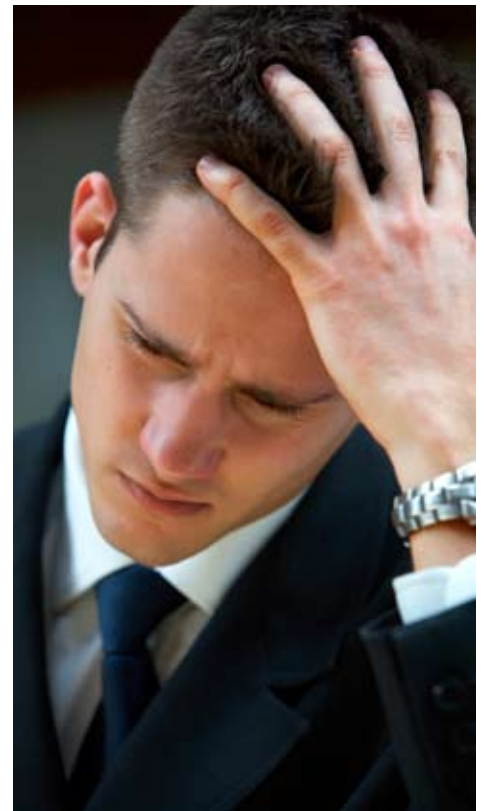
view to committing large-scale internal frauds. Strong pre-employment vetting is crucial to address this threat. Another common employee fraud among general insurers is the facilitation of fraudulent claims payments, usually by adding unauthorized payments to existing claims or by reopening and paying out on old ones, often within self-authorization limits.

Meanwhile, bribery and corruption are currently receiving extensive law enforcement attention worldwide. The number of Foreign Corrupt Practices Act (FCPA) investigations and the severity of resultant fines and prison sentences are increasing. In addition, the British government has proposed a new Bribery Bill. This increased focus means that insurers need to have properly implemented programs which will let them answer three fundamental questions if any employee is found to be involved in bribery and corruption:

- What did you do to reduce the risk of this happening?
- What did you do when you suspected it had?
- What did you do once you knew for certain?

Where offenses are suspected, companies must ensure that independent investigations occur and, if suspicions prove correct, appropriate action is taken against the guilty and appropriate disclosure is made to the authorities.

Money laundering and sanctions will also continue to attract substantial attention for the foreseeable future. Most insurers have mature controls in these areas, although some general insurers still grapple with sanctions legislation due mainly to various contractual arrangements under which they lack access to payee or customer details. Insurers cannot afford to reduce their focus here, given ongoing governmental interest.



With so many issues to consider, the following risk mitigation strategies should get top priority:

- Robust employee screening;
- Data security from both internal and external threats;
- Transaction monitoring for anomalies which may indicate money laundering, corruption, or other fraud;
- Facilities through which employees can report all suspicions of wrongdoing – anonymously if required – and the capacity to investigate resulting information independently of the business areas involved;
- Appropriate due diligence on customers and suppliers;
- Staff training in all areas of fraud prevention, particularly for senior management who set the tone for the organization.

We will never remove all financial crime from any company, but implementing these strategies can help reduce it.



Brendan Hawthorne joined Kroll's London investigations team this year as managing director, bringing with him more than 16 years of experience in forensic and financial investigations. He qualified as a Chartered Accountant with a big four accounting firm and has worked on many large and high profile investigations. Prior to joining Kroll Brendan headed up the financial crime team in a global financial services organization based in the UK



The pitfalls of arbitration

Asuncion C. Hostin & Annie Cheney

Businesses are increasingly turning to arbitration to settle disputes: according to the American Arbitration Association (AAA), the total number of cases filed in 2008 rose to 138,447 – up 8 percent from 2007. In the same period, foreign cases filed with the AAA's International Center for Dispute Resolution jumped 13 percent. Of all the cases filed with the AAA in 2008, a significant proportion involved employment and construction disputes.

Touted as an attractive alternative to expensive and time-consuming litigation, arbitration is not without drawbacks. Its emphasis on speedier results and cost effectiveness may impede a party's ability to present evidence and defend itself. Unlike litigation, arbitration also severely limits discovery and results in binding judgments with extremely few grounds for appeal. The role of electronic discovery is also murky. Common e-discovery issues raised in arbitration are the production of documents, time and cost burdens, privilege waiver and "claw-back" agreements. However, the ultimate

decision on whether to allow e-discovery depends on what the particular arbitrator decides. In this, as indeed in all questions at issue including the main point of dispute, arbitrators are not bound by rules of law, but may base their decisions on broad principles of justice and equity.

Most important, arbitration is, fundamentally, a business. As the court explained in *Britz, Inc. v. Alfa-Laval Food & Dairy Co.* (1995), "even though state and federal policy favors private arbitration and the AAA is certainly a respected forum for such arbitration, the AAA nevertheless is a business enterprise 'in competition not only with other private arbitration services but with the courts in providing – in the case of private services, selling – an attractive form of dispute settlement. It may set its standards as high or as low as it thinks its customers want.'"

Arbitration presents particular challenges in disputes where fraud is involved or suspected. The limitations imposed on discovery, for example, may discourage parties from conducting independent investigative due diligence, even in disputes where fact finding is essential to a favorable outcome. In the construction sector,

companies facing an arbitration claim may overlook the need to investigate vendors or subcontractors who performed related work.

This could be a costly mistake: in the Kroll Global Fraud Survey 2009 25 percent of firms reported suffering vendor or procurement fraud in the previous three years.

The individual arbitrator can also present problems. Most institutions require impartiality and that arbitrators disclose any ties that would compromise their independence. In such disclosures, however, arbitrators may not be thorough, omitting relevant information or even misjudging the significance of a given professional experience. In *O'Flaherty v. Belgum*, for example, an AAA arbitrator failed to disclose that he had once been the plaintiff in a dispute in which the claims mirrored those at issue in the case he was arbitrating. The parties did not learn of this conflict until after he rendered his decision. Likewise, in *Azteca Construction, Inc. v. ADR Consulting, Inc.*, an arbitration award was vacated by an appellate court as a result of a challenge to the impartiality of the chosen arbitrator. The court noted that because they wield such mighty and largely unchecked power, the neutrality of arbitrators is of crucial importance and should not be left to the unfettered discretion of a "private business," such as the AAA.

These issues are causing companies to carefully consider whether to enter into arbitration, and to gather evidence through investigations that could be classified as "extrajudicial discovery." Given the complexities and problems of arbitration, conducting swift and targeted research of the counterparties, arbitrator, and the circumstances underlying the claim is essential.

Asuncion C. Hostin is a managing director of business intelligence and investigation. A former Assistant U.S. Attorney for the District of Columbia, Sunny has expertise in the investigation and prosecution of complex criminal matters. Prior to this, Sunny was a staff attorney for the Antitrust Division of the Department of Justice where she investigated and litigated anticompetitive mergers and acquisitions. She has lectured extensively on labor and employment and white-collar crime issues and instructed on evidence at Pace School of Law. Sunny regularly contributes to CNN, Tru TV, Fox News, and Fox Business Channel.

Annie Cheney is a director in the New York office. Prior to joining Kroll, she worked as a freelance journalist, producing radio documentaries for National Public Radio and for magazines such as *Harpers*. Her work received the Deadline Club Award for Best Feature Reporting by the Society of Professional Journalists in 2005. Annie is the author of *Body Brokers: Inside America's Underground Trade in Human Remains* published in 2006.

Tackling client and data problems

Tracey Stretton & Mark Surguy

An old threat

The professional services sector may experience less fraud than others, but there is still plenty around. In the UK, the Serious Fraud Office recently prosecuted several solicitors for mortgage fraud. In the same country, not so many years ago, the senior partner of a small accounting firm forged a client's signature on a series of stock transfer forms. His innocent fellow partners were found liable as well. The latter case followed a substantial fraud in Dubai involving a firm of London solicitors: one of its partners had allegedly drafted consultancy contracts which facilitated a massive fraud by the firm's client. The allegations were withdrawn, but the firm's insurers still made a substantial settlement payment. They in turn sought a contribution from the innocent partners. The court established that the dishonest partner had acted in the course of the business of the firm, thereby rendering the innocent partners liable.

Cases like these may be on the rise in today's economic environment. Kroll's annual fraud survey revealed that professional services experienced one of the strongest up-ticks in fraud over the last 12 months.

In some cases desperation is heightening the risks.

For example, the moment an employee thinks redundancy

is a possibility, the employer faces a greater danger of data theft, of customer lists, trade secrets, research data, or price sensitive information. It also remains to be seen whether the increased regulation promulgated early this decade in the wake of the Enron scandal will truly eliminate so-called "cozy relationships," where audit and accountancy firms succumb to client pressure to "make the numbers work." The last six years have seen considerable merger activity and the pressure to mis-state the accounts of struggling companies may well be high.

As the initial examples in this article illustrate, however, perhaps the biggest risk for the professional services sector is to be drawn into a client's fraud. Recent incidents abound:

- India's largest fraud in 2009, of IT outsourcing firm Satyam Computers, involved the company's auditors, who allegedly signed mis-stated accounts knowingly in return for a larger than normal audit fee. The audit firm has been joined to several lawsuits, and two partners have been arrested.
- One of the most senior partners at a New York law firm was recently convicted over the collapse of a commodities broker. Now that firm has been drawn into litigation.
- The principal of another New York law firm became involved in fake security transactions and the partnership has collapsed into bankruptcy.

The recent popularity of the Limited Liability Partnership (LLP) may help reduce the danger in practice, depending

on the terms of the partnership agreement. Even if it does, however, the reputational implications of client fraud remain significant. After all, Arthur Andersen – an LLP in the United States – was cleared of all wrongdoing in its association with Enron, but its business nevertheless disintegrated and its brand was fatally tainted.

Moreover, the need to pursue compensation for fraud is also greater when finances are tight. In the past, cases of fraud might have been overlooked and the losses absorbed. Now, aggressive pursuit of redress in the hope of recovering some proceeds is much more likely, putting even the innocent at greater risk.

A new threat

As the professional services sector adopts new technologies and ways of working, new risks arise. The Internet and e-commerce have brought substantial business benefits, but also a sharp increase in the incidence of "e-fraud" in particular, and commercial fraud in general. In Britain alone, companies now lose in excess of \$16 billion a year because of cyber crime and data theft. Ninety one percent of respondents in a recent UK survey cited cyber crime as a major business risk, resulting in lost customers, damaged brands, and lawsuits.

According to Kroll's annual fraud survey, over a quarter of companies in the professional services sector were hit by information theft in the past three years, making such attacks – along with theft of physical assets which affected the same number – the most widespread fraud threat. Losing valuable data brings the risk of losing clients and money as well. Professional services firms also risk breaching the duty of confidentiality owed to clients and the responsibility to keep clients' data secure in order to protect them from fraud.

Information management amid rapid technological advancement brings many and varied challenges. The modern thief can steal more with a computer than with a gun. The days of copying a few company secrets onto a floppy disk are long gone. Increasingly complex networked environments recognize no physical boundaries, and permit a multitude of devices to communicate and interact. These new technologies enable quick, quiet data theft on a massive scale. A thumb-sized USB drive, for example, can store the equivalent of four tons of paper documents; email can send information away instantly; gigabytes of data from desktops or servers can be burned covertly onto DVDs and PDAs; and wireless networks and Bluetooth devices increase the risk by making data access and transportation easier still.

The law and business respond

The law has not developed sufficient new rules to meet the challenges of these cyber crimes. Instead, existing procedures and remedies are being applied in new contexts. Freezing and search orders are available in common law regimes, and English courts have the power to order an innocent party caught up in wrongdoing to disclose the identity of a wrongdoer. Data does not respect jurisdictional boundaries, however, and so the applicable law in the event of fraud is never obvious.

Unlike the law itself, the context in which it is being applied has changed beyond recognition. Huge volumes of electronically stored material often have to be reviewed to establish a legal remedy. Moreover, this electronically stored information can also be readily copied, and therefore moved without permission; altered, and therefore falsified; and the identity of the author can be easily concealed or assumed by anyone with access to a user's password. This makes the authenticity of the evidence much less reliable and the risk of not finding it, or contaminating it, high. It has become essential for fraud lawyers to work with investigators and computer forensic experts to uncover evidence and preserve its integrity so that it will be admissible in court.

If significant volumes of electronic information create the risk of unauthorized access and even information leakage, professional service firms should determine what information they hold, where it is, and who has access to it. A computer use and document management policy is only part of the solution. Enforcing the policies and refreshing them regularly is essential. The concept of e-health is also beginning to

spread, where organizations purposefully delete masses of data and store only what they need for business purposes. Such firms carry a much lower risk of being saddled with fraud.

The professional services sector is not exempt from fraud, but often has less direct control. In the current economic environment, it faces heightened risks, especially that of being drawn inadvertently into the fraud of clients. The ongoing exploitation of information technology's benefits also brings a dark side of increased vulnerability to certain crimes. Professional services organizations need not only to be aware of all these risks but, like other companies, have the right security controls and incident response plans in place.



Tracey Stretton is a legal consultant at Kroll Ontrack. She is an expert in the management of electronic information and legal technology. Before joining Kroll, Ms Stretton practiced as a solicitor in South Africa and Australia working primarily on complex commercial litigation cases. She speaks regularly at conferences and has written numerous articles on the impact of technology on law and business and is a contributing author to the book *Electronic Evidence and Discovery – What Every Lawyer Should Know Now*, released by the American Bar Association this summer.



Mark Surguy is a legal director in the Dispute Resolution & Litigation Group at Pinsent Masons LLP and leads the firm's fraud practice. After undergraduate studies at Cambridge University he qualified as a Solicitor in 1988. Mark writes and speaks about the risks to organizations of holding large volumes of electronically-stored information. He also contributes to LexisPSL's *E-Disclosure Practice Notes* and is currently the chairman of the Midlands Fraud Forum.

EIU SURVEY

Although still facing only low absolute losses, professional services firms may need to consider doing more to address their fraud problems, especially given the role of these businesses in the growing battle against financial crime.

Fraud levels, a complex story: On the surface, the numbers look good, but digging deeper reveals a more nuanced story.

- The average loss per company over the last three years was \$2.9 million, which is well below the average. It is over twice the 2008 survey figure – \$1.4 million – but nevertheless an extremely good result.
- Moreover, the vast majority of professional services respondents are from smaller companies – those with annual sales of under \$5 billion. These businesses averaged a loss of only \$4.6 million, so size only partly explains these low losses. More worrying, smaller companies as a whole saw average fraud losses decline last year, contrary to the trend in professional services.
- 28% of sector companies saw an increase in the level of fraud at their company in the last year, the second-highest proportion, and greater than the 24% who saw a decline.
- Although, as a sector, professional services had the second-lowest proportion of companies hit by fraud (77%), and the lowest incidence of theft of physical assets (27%), it still had the second-highest rate of information theft (27%) and money laundering (7%).

The response is sometimes wanting: Sector companies do not always recognize and rise to the challenge.

- These firms are less likely to feel at risk to specific types of fraud, which can create blind spots. For example, only 4% think themselves highly vulnerable to internal financial fraud, yet 16% suffered from it in the last three years.
- Professional services companies are also less likely than average to deploy any of the anti-fraud methods listed in the survey, with the exception of due diligence, where the number is only slightly above average (48% compared with 46%). Only 58% have information security measures in place, compared with an average of 71%, even though information theft is a marked problem.

A smaller than average fraud problem is not the same as no fraud problem. Professional services firms need to address the weaknesses they do have, especially in information security, so that losses do not grow.

Written by The Economist Intelligence Unit

REPORT CARD PROFESSIONAL SERVICES

Financial Loss: Average loss per company over past three years \$2.9 million (33% of average)

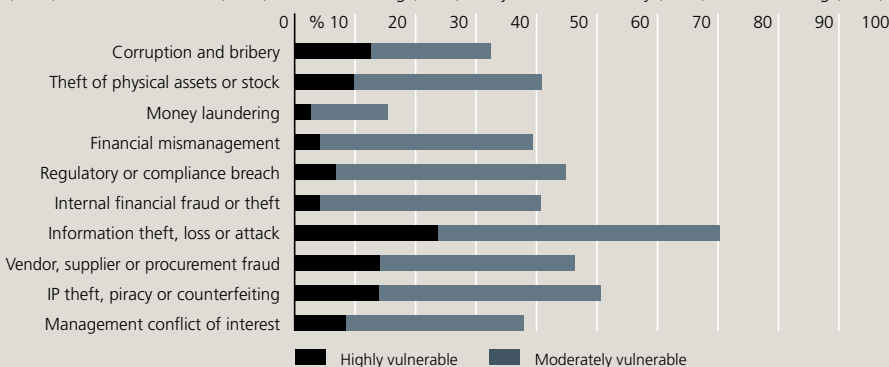
Prevalence: Companies suffering fraud loss over past three years 77%

Increase in Exposure: Companies where exposure to fraud has increased 86%

High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable to specific frauds
Information theft, loss or attack (24%) • IP theft, piracy or counterfeiting (14%) • Vendor, supplier or procurement fraud (14%)

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in last three years
Theft of physical assets or stock (27%) • Information theft, loss or attack (27%) • Management conflict of interest (23%) • Regulatory or compliance breach (21%)

Investment Focus: Percentage of firms investing in this type of fraud prevention in the next year: IT security (42%) • Financial controls (38%) • Staff screening (38%) • Physical asset security (35%) • Staff training (34%)



NORTH AMERICA OVERVIEW

North America continues to show the lowest number of frauds among regions in the survey, with only 80% of companies having suffered at least one fraud. However, specific categories of fraud saw significant increases over the past year.

- For seven out of ten categories of fraud in the survey, the percentage of respondents who experienced fraud in the last three years was up on the 2008 findings. In several cases, these increases were substantial: the number reporting internal financial fraud rose from 10% to 15%, and that for financial mismanagement increased from 16% to 23%.

The region is also no longer the clear low-fraud-leader. In last year's survey, it had the lowest incidence for eight out of the ten frauds; this time around it has that distinction for only three – theft of physical assets (33%), corruption (13%), and vendor fraud (11%).

- In the current survey, North America reported the largest proportion of companies experiencing more fraud due to the financial crisis than in any other region (32%).
- In addition to the three types of frauds where North America fared better than other parts of the world, the region also experienced the second lowest incidence in four other categories: information theft (23%), management conflict of interest (22%), regulatory breaches (18%), and internal financial fraud (15%).
- The number of companies suffering at least one fraud, 80%, was also the lowest globally.
- Most important, the average cost of fraud to regional companies, although still above the survey average, was \$12.0 million, down from \$15.1 million last year.

Concern about fraud, on the other hand, has unmistakably risen.

- The proportion of companies that consider themselves highly vulnerable to nine out of ten frauds in the survey has either risen – in seven categories – or stayed the same compared to the 2008 results. The only exception is IP theft, where the figure declined from 17% to 14%.
- For three of these frauds, more North American companies consider themselves highly exposed than in any other part of the world: regulatory breach (17%), management conflict of interest (16%), and money laundering (6%). This is even though the incidence in North America is low compared to elsewhere for these three areas

Spotlight on Canada

Because of the large preponderance of United States respondents in the North American sample, the figures for that country and the region differ very little. Canada, on the other hand, has some distinctive features. This year, the overall incidence of specific frauds, and also their relative growth or decline since the previous survey, roughly tracked that of the region as a whole. On the other hand, Canadians are less worried. For every fraud but money laundering – where the difference is slight – fewer Canadian companies than American ones say they are highly vulnerable. For financial mismanagement, this is particularly stark (4% of Canadians compared to 15% of respondents from the United States), even though incidence of the fraud itself was



higher last year in Canada (25% compared to the US figure of 22%). Canadians are accordingly less likely to invest in anti-fraud strategies than their neighbors, with 18% planning no such spending next year, compared with 9% in the United States.

	2009	2008
Financial Loss: Average loss per company over last three years	\$12.0 million (137% of average)	\$15.1 million (184% of average)
Prevalence: Companies suffering fraud loss over last three years	80%	79%
High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable	Information theft, loss or attack (21%) Regulatory or compliance breach (17%)	Information theft, loss or attack (21%) IP theft, piracy or counterfeiting (17%)
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in last three years	Theft of physical assets or stock (33%) Information theft, loss or attack (23%) Financial mismanagement (23%) Management conflict of interest (22%)	Theft of physical assets or stock (28%) Information theft, loss or attack (22%)

- 84% of companies reported that their exposure to fraud had increased – the highest survey figure.

This concern is not, however, translating into more widespread investment in fraud prevention.

- Perhaps because of its relatively low rates of fraud, the proportion of North American companies that have adopted nine of the ten anti-fraud strategies in the survey is

below average, and in six cases they are less widespread than anywhere else.

- The exception in both cases is staff background screening, which 52% of North American firms use, the highest in the survey.

Overall, in North America, fraud has not become the problem it is elsewhere and investment in fraud prevention strategies has yet to match the level of concern.

EUROPE OVERVIEW

European companies are confident about their exposure to fraud, having invested widely in anti-fraud measures.

- For every fraud covered in the survey, fewer Europeans consider themselves highly vulnerable than the overall average. In two cases – information theft (16% describe themselves this way) and management conflict of interest (6%) – these are the lowest figures for any region.
- Europe also has the highest proportion of companies that believe their exposure to fraud has not increased (30%).
- This confidence may come from widespread use of anti-fraud measures. Of the ten strategies listed in the survey, nine were more common in Europe than average – the only exception was staff background screening, which just 32% have in place. Six of these measures – IT security (83%), physical asset security (78%), management controls (72%), reputation protection (48%), risk management systems (47%) and IP monitoring (43%) – were more common in Europe than anywhere else.
- The decrease in financial loss from fraud does not necessarily translate to there being a decreased threat; one might argue that companies have responded to these very real threats and are investing in processes and actions needed to address the causes.

The results of these anti-fraud efforts, however, are middling, and in some cases confidence in them may be misplaced.

- Despite its widespread use of anti-fraud strategies, the proportion of European companies hit by nine out of ten of the frauds covered in the survey is within three percentage points of the survey average, and in five cases the difference is under 1%.
- Regulatory or compliance breaches constitute the only fraud to vary significantly from the norm, but here Europe has a higher proportion of firms that have suffered in the last three years (25%) than any other region.
- Nor has there been much change from last year. The average loss over the last three years, \$7.7 million, is slightly down from the 2008 figure, but the number of companies suffering from at least one fraud rose to 89%, again the highest in any region. Meanwhile, six of the frauds in the survey saw an increase in incidence from the 2008 figures, and four a decrease. Once more, the changes were small.

European confidence in corporate anti-fraud efforts might leave it ill prepared to face new challenges.

- To cite one example, the region has a higher than average rate of management conflict of interest in the last three years (25%), but the lowest number of companies calling themselves highly vulnerable (6%), as well as the fewest spending on further management controls in the coming year (25%).
- More broadly, over the next year, fewer companies in the region will invest in every anti-fraud strategy covered in the survey than the global average. In five cases, spending will be less widespread here than anywhere else.
- Meanwhile, the other issues are making life harder. The continent had the highest proportion of respondents indicating that entry into new markets had increased vulnerability (28%), and that reduced revenues had done the same (16%).
- The decrease in fraud does not necessarily translate to there being a decreased threat, but more that there is more investment in battling the causes. Companies have responded to the very real threats and are investing in processes and actions needed to address.
- While the results might suggest that European companies are relatively content with their fraud measures, Kroll's experience suggests that however effective the controls, they can be

Spotlight on United Kingdom

This year the United Kingdom saw less of most kinds of fraud. Fewer British firms than the European average suffered from eight out of ten of the frauds covered in the survey. For the two exceptions, theft of physical assets and internal financial fraud, the differences were small. Moreover, the average loss per company, \$3.8 million was about half the European average. On the other hand, the problem was more spread out, with 90% of British companies experiencing some type of fraud in the last year, slightly more than for the region as a whole.

circumnavigated by collusion and organized fraud. Rarely do we see major frauds identified by prevention controls; they are usually uncovered by accident, by whistleblowers and often when it is too late. The findings might indicate that corporates are lulling themselves into a false sense of security with compliance procedures and relying on regulations to capture misconduct.

European companies have certainly taken measures against fraud, but the results are less than they might be entitled to expect.

	2009	2008
Financial Loss: Average loss per company over last three years	\$7.7 million (88% of average)	\$8.3 million (101% of average)
Prevalence: Companies suffering fraud loss over last three years	89%	84%
High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable	Information theft, loss or attack (16%) Theft of physical assets or stock (13%)	Information theft, loss or attack (25%) IP theft, piracy or counterfeiting (15%)
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in last three years	Theft of physical assets or stock (38%) Management conflict of interest (25%) Regulatory or compliance breach (25%) Information theft, loss or attack (22%) Financial mismanagement (22%) Vendor, supplier or procurement fraud (21%)	Theft of physical assets or stock (34%) Regulatory or compliance breach (29%) Management conflict of interest (24%) Information theft, loss or attack (23%) Corruption and bribery (22%) Financial mismanagement (20%)

Tackling compliance with conviction

David Robillard

Through many years of investigating corporate malfeasance in Mexican-based manufacturing companies, we have observed that firms which make integrity programs an inherent part of their

cultures are far more effective at detecting and preventing fraud. In today's post-Sarbanes-Oxley world, integrity programs have become de rigeur. Too many companies, though, consider these simply a compliance requirement, not the right or smart thing to do. A purely compliance-based approach is not enough: focusing

solely on rules does not motivate workers; it scares them. Integrity programs must be implemented with conviction from the executive level down.

Below are examples that illustrate how two companies approach integrity. Although both describe Mexican-based operations, the lessons apply globally.

An auto parts manufacturer, has gone beyond Sarbanes-Oxley to expand the traditional role of the audit. A Special Investigations Group reports to the CEO, who in turn chairs the Integrity Committee – composed of Directors from Administration, Audit, Human Resources, Finance, and Legal. The group is trained in a range of investigative methods, including computer forensics, investigative interviewing, and data mining, and has been building its capabilities for over ten years. To support the team's work, the company established an integrity line through which the audit department receives all reports of misconduct. Over time, it has developed the capacity to deploy resources swiftly on a range of issues, including conflict of interest, FCPA violations, corrupt practices, discrimination, harassment, financial fraud, unsafe working conditions, and substance abuse.

The company has a seven day maximum response time to classify reports and

REPORT CARD MANUFACTURING

Financial Loss: Average loss per company over past three years \$7.4 million (84% of average)

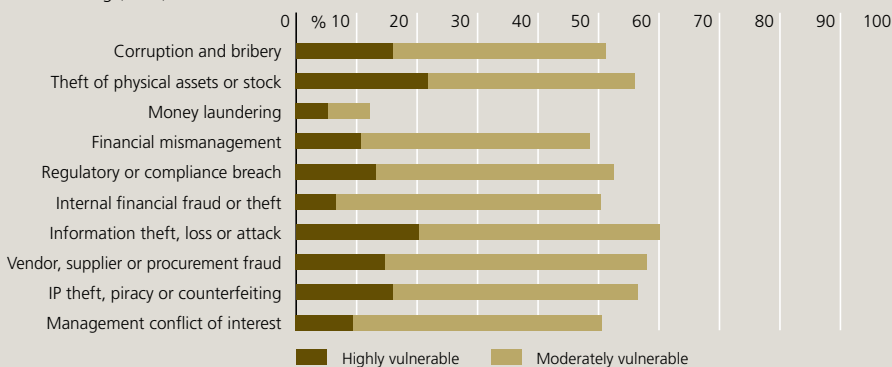
Prevalence: Companies suffering fraud loss over past three years 89%

Increase in Exposure: Companies where exposure to fraud has increased 80%

High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable to specific frauds
Information theft, loss or attack (21%)

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in last three years
Internal financial fraud or theft (24%)

Investment Focus: Percentage of firms investing in this type of fraud prevention in the next year:
Staff training (31%)



EIU SURVEY

Losses are down but concerns remain: This year's survey indicated that the manufacturing industry had seen fraud losses decline, but also pointed to two particular areas of concern: financial mismanagement and IP theft.

- The average loss per company over the last three years declined from that of the previous survey, both in absolute terms – to \$7.4 million from \$8.5 million – and in comparison to the overall average, to 84% from 104%.
- Although the incidences of most types of fraud in this sector were near the overall survey averages, 30% suffered from financial mismanagement in the last three years, well up from the 2008 survey (17%).
- The industry also saw the highest level of IP theft over the last three years (22%), up from 18% in the previous survey. The ongoing problem in this area explains why manufacturers have the second-biggest percentage of respondents who feel highly vulnerable to IP fraud (16%).

Serious efforts: Some of the reduction in fraud losses is a result of the industry taking the problem seriously.

- More manufacturing companies deploy seven out of ten of the anti-fraud strategies listed in the survey than average: 80% have management controls, the highest proportion of any industry. 81% have physical security systems and 53% have vendor due diligence programmes.
- Moreover, 39% of companies are investing further in due diligence, the most of any industry.

The downturn may have a silver lining: As with some other industries, however, the downturn may be raising vulnerability to fraud while making less available to steal.

- 27% say that the global financial crisis has increased fraud levels at their organization, while 20% say reduced revenues on their own have heightened vulnerability – the highest figure for any industry. Meanwhile, for 37% entry into new, riskier markets, often driven by the demands of the current environment, has also raised exposure to fraud – the second-highest sector figure.
- The number of companies that considered themselves highly vulnerable increased on last year's figures, more than doubling for three categories – theft of physical assets (8% compared with 22%); corruption and bribery (6% compared with 16%); and money laundering (2% compared with 5%)
- Even while perceived vulnerability has been rising, however, in the last year only 19% say they have seen an increase in the level of fraud, compared with 37% who have seen a decline. Just as the industry is having a tough time finding profits, it is likely that fraudsters are having a hard time finding money to pilfer.

Overall, manufacturing companies have made some headway with fraud, although financial mismanagement and IP theft remain significant issues. How much of this success is a result of their own efforts, and how much from the broader effects of the downturn, will only become clear in an economic recovery.

Written by The Economist Intelligence Unit



determine the best method to proceed. Compliance-focused cultures, on the other hand, tend to get bogged down at this point, specifically in judging which reports merit investigation and which are nuisances, as well as in deploying investigative resources efficiently. Next, once allegations are proven, the company takes swift decisions in addressing guilty parties. Recently, a senior executive with more than 15 years tenure was terminated with cause, despite his strategic importance to the company. Immediately afterwards, the decision and the reasons for it were communicated to every employee. The impact was swift and reinforced a culture of integrity and accountability.

A United States-based manufacturer of medical devices, provides an example of a program that works less well. For years, Mexican manufacturing has been synonymous with maquiladoras, facilities originally created to make products with parts imported duty free. This firm operates such a plant in Mexico. A routine audit there uncovered more than \$1 million waste of raw materials. Within three weeks of this report becoming known, two senior plant employees who had initiated an internal investigation – the HR Manager and the Quality Control Supervisor – were murdered. The client sought Kroll's assistance to determine if these incidents were related.

Because the company's United States-based integrity program is not used at the local operation, our work and that of the company's auditors was made much more difficult. In practice, the operation is disconnected from head office oversight. An integrity line exists, but employees are unaware of it. The line also has no Spanish speakers, making it useless in Mexico. Local managers maintain tight control over communications going outside the plant. Staff members fear expressing any concerns, greatly reducing their value as sources of information.

More than ever, companies need to integrate integrity programs into their corporate cultures to enable a greater flow of information from staff on misconduct. This may not make an organization bulletproof, but it will allow much swifter problem identification and decision making.



David Robillard is Kroll's country manager in Mexico. He advises clients on reputational and corporate risks and has done so for over 15 years. Previously David was a market intelligence specialist for ICA Fluor Daniel, a Mexico-based joint venture and leading provider of industrial engineering, procurement and construction services in Latin America.

The United Kingdom's new anti-bribery legislation



Companies need to be aware that new regulation also covers consultants and agents says Richard Abbey

Corruption remains a major risk issue for international businesses. Companies may face pressure to engage in unethical or corrupt practices in many emerging markets – and some developed ones – but they are also seeing increased scrutiny from regulators and governments who are making a priority of stamping out corruption within the global economy.

In the past, the United Kingdom has been criticized for its attitude toward the prosecution of companies and individuals responsible for corrupt acts within its borders and abroad. British corporations, their directors, and overseas entities doing business in the country, however, will soon see a major change in attitude from the authorities. Richard Alderman, head of the Serious Fraud Office (SFO), has clearly indicated his office's commitment and determination to investigate and punish entities found guilty of bribery. Several United Kingdom companies and individuals have been prosecuted or fined in the past year, and the SFO is actively encouraging whistleblowers to provide evidence of the wrongdoing, as opposed to just reporting it.

More important, the SFO is taking great steps to persuade companies aware of involvement in corrupt acts to “self report” – a model already used by authorities in the United States. In return for self-reporting, businesses receive more lenient disciplinary treatment than if the SFO becomes aware of the offense through other means. How successful this approach will be remains to be seen. Therefore, some organizations appear willing to take the risk of the issue not being uncovered. As the SFO makes examples of more firms, however, this attitude might change.

The Government has also published details of a draft Bribery Bill, which, if passed, will come into force in 2010. The bill currently sets out the following general offenses:

- to offer, promise, give, or request an advantage;
- to agree to receive or accept an advantage;
- a specific offense of bribery of a foreign public official;
- negligent failure by a commercial organization to prevent bribery.

The maximum penalty in the first three offenses is ten years imprisonment. In the last offense, the penalty is the imposition of an unlimited fine. The bill also contains an extra-territorial jurisdiction clause to enable the prosecution of bribery committed abroad by United Kingdom residents, nationals, and companies.

The Bribery Bill sets out that the fourth offense will take place when:

- a person performing services for the commercial organization bribes another person;
- the bribe is in connection with the commercial organization's business; and
- another person connected within the organization with responsibility to prevent bribery negligently failed to do so.

Importantly the person offering the bribe need not be an employee, as the law would also apply to consultants or agents.

Corporate directors will need to put in place adequate controls and procedures in order to demonstrate that all reasonable steps have been taken to prevent or minimize the opportunities for corrupt payments by employees or agents. Advisable steps may include, but not be restricted to:

- implementing a robust compliance program which states the company's attitude and policy toward corrupt payments, and communicating this to all staff, agents, consultants, and contractors globally;
- regularly training staff in the relevant national regulatory acts and internal compliance policies;
- demonstrably maintaining adequate books, records, and internal controls at all subsidiaries to minimize the risk of corrupt payments;
- maintaining a clear trail of due diligence and vetting of agents and consultants used to win business; and
- conducting regular risk audits of sales departments dealing with high risk business opportunities or operating in high risk jurisdictions.

The United Kingdom is tightening up its anti-bribery regime. Companies need to take note.

Richard Abbey is a managing director and head of financial investigations in London. He specializes in managing complex and multi-jurisdiction frauds and international bribery and corruption investigations and is currently leading the investigation into the collapse of Glitnir Bank in Iceland. He is a qualified accountant and prior to joining Kroll worked at one of the big four.

Not all identity theft is high-tech, and no one is immune



Criminals are finding new ways to steal identities, including targeting employees says Brian Lapidus

Scores of articles have breathlessly recounted how Anna Bernanke, wife of United States Federal Reserve Chairman Ben Bernanke, had her purse stolen and the subsequent check fraud. The inevitable conclusion: it can happen to anybody! Identity theft is the fastest growing crime in both the United States and Canada. It is the leading cause of consumer complaints to the American Federal Trade Commission, with cases totaling 313,982 in 2008. In Canada, it is estimated that one in ten have become victims of identity theft.

High profile cases, however, often obscure the reality of identity theft. The real focus of the story should have been the members of Cannon to the Wiz, a Chicago-based ring that perpetrated both high- and low-tech thefts of identities and financial information. The ring had been in the view of law enforcement well before the Bernanke incident. In April 2009, Detroit police arrested four members of the ring who were targeting fans at a sporting event. In June, Virginia federal prosecutors charged 10 with conspiracy and bank fraud, and, just as summer was winding down, authorities arrested a check casher from the ring in Miami.

To identity thieves, everyone is reduced to valuable information such as Social Security or Social Insurance numbers, credit card

numbers, addresses, and dates of birth. Data can come from practically any source. While most news stories highlighted the Cannon's pick-pocketing activities, the ring also infiltrated offices, including those of a United States sponsored charity and the offices of a doctor, in order to obtain checks from the mailroom, personal identification information from medical files, and credit card details.

The Cannon's activities are a wake-up call to organizations. First, data security cannot be left to the IT department alone. This fosters the belief that anti-virus software, firewalls, and other cyber security measures will effectively eliminate the risk of a data breach. Frequently, the breaches occur due to careless or disgruntled employees, or to employees who are simply unaware that their actions violate security protocols. According to a 2008 Ponemon study, over 88 percent of data breaches involved insider negligence. The per-victim cost of these was \$199 per record; those traced to malicious acts cost \$225 per record.

Second, never assume that low-tech methods mean that the identity thief is a novice. Authorities reported that members of the Cannon often met for seminars to learn more effective tactics. They used advanced equipment to manufacture fake identification and employed complicated check fraud schemes to drain victims' bank

accounts. They took – according to court documents in the federal case – some \$2.1 million from ten different financial institutions. Thieves generally look for the easiest means of access. Once on the inside, they quickly recognize the constant business struggle to secure information contained in items like incoming mail or paper files that are often highly accessible to employees. Missing hardcopy files or a lost office key should not be dismissed as petty; these merit diligent investigation.

Finally, organizations must take background screening efforts seriously. News reports indicate that one of the thieves worked with a corrupt employee at a doctor's office, and federal informants from the ring indicated that the standard was to pay anywhere from \$200 to \$500 for a set of complete personal information. Background screening is no panacea, but a thorough check performed by a reputable third party brings all sorts of information to light: criminal histories, financial histories, and professional misconduct to name a few. Data rich organizations, like the doctor's office, are prime targets and thus have an obligation to perform thorough background checks.

It is unfortunate that Ben and Anna Bernanke had their personal information stolen. Perhaps the one positive outcome is that the incident can encourage discussion of the prevalence and true nature of this crime.

Brian Lapidus is chief operating officer of Identity Fraud Solutions based in Tennessee. He leads a team of investigators in ID theft discovery, investigation and restoration, including helping corporations to safeguard against and respond to data breaches.

A glimpse into Mexico's shadow pharmaceutical market

Guillaume Corpart, Manuela D'Andrea & Enrique Orellana

Amid Mexico's recent influenza pandemic, the real danger that fake medication could imperil the health of the population was acknowledged. The country's health ministry warned the public of the risks of buying medications, such as Tamiflu and Relenza, online. Armed guards protected warehouses storing medications. Pharmacies and hospitals maintained strict

vigilance and were asked to keep faultless inventory records to avoid theft.

These measures helped with a crisis, but the same underlying threats besiege the industry every day. Kroll recently conducted an in-depth investigation into the growing problems afflicting this sector in Mexico. Here are some of the key findings.

The country's pharmaceutical industry faces substantial fraud risks. The \$15.5 billion market is plagued by widespread

and difficult-to-tackle problems – counterfeit goods, theft, and irregular sales practices chief among them. Overall, illicit activity amounts to about \$1.9 billion per year, or 12 percent of the formal market. Counterfeiting affects all companies and represents 81 percent of the illicit market. Theft – including stealing from pharmacies and warehouses, cargo theft, and pilferage – constitutes an additional 12 percent, while the illegal sale of drug samples accounts for 5 percent.

Counterfeit drugs

Sales of counterfeit drugs in Mexico were estimated to exceed \$1.5 billion in value in 2008, or 10 percent of the formal market. They are the product of a complex and lucrative shadow industry with a global reach. Well coordinated rings, often working closely with organized crime, slip fake medication into Mexico's legitimate drug supply. Such shadow players replicate operations parallel to the legitimate industry, including importing, manufacturing, packaging, and distributing their false merchandise. Counterfeiting usually takes place in small laboratories, often located in residential buildings, supported by an entire network of suppliers and intermediaries. Legitimate business activities can be used as a front, while in other cases fictitious corporations or ghost companies provide cover.

Two types of counterfeiting practices are rampant in Mexico:

- **Partial or total product substitution:** Counterfeit medication often includes the original active ingredient but in a smaller dosage than indicated on the packaging, thus creating a sub-potent drug. Even when the active ingredient is present, the medication may still be laced with potentially hazardous material. In one case, counterfeit pills for erectile dysfunction were found to have traces of LSD, a semi-synthetic psychedelic drug.
- **Repackaging of expired drugs:** Criminal rings also acquire expired medicine in order to repackage it and then reinsert it into the distribution channel. The absence of a formal waste management system for expired drugs makes this "recycling" easier.

The growing presence of illicit, online pharmacies is further increasing the proliferation of counterfeit medication. In 2004, the United States Drug Enforcement Agency found over 200 online pharmacies operating along the United States-Mexico border. It is calculated that these businesses sent over 11 million pills to American buyers between 2003 and 2008. Furthermore, over two percent of Mexico's 110 million inhabitants are said to have purchased

REPORT CARD HEALTHCARE, PHARMACEUTICALS AND BIOTECHNOLOGY

Financial Loss: Average loss per company over past three years \$11.7 million (133% of average)

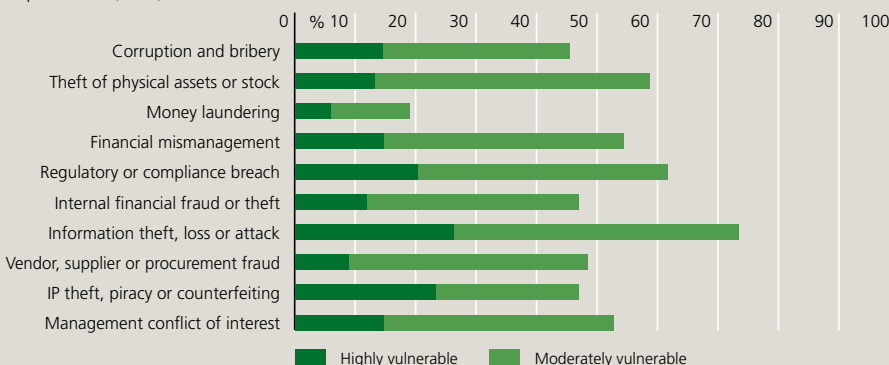
Prevalence: Companies suffering fraud loss over past three years 88%

Increase in Exposure: Companies where exposure to fraud has increased 71%

High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable to specific frauds
Regulatory or compliance breach (21%)

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in last three years
Information theft, loss or attack (21%)

Investment Focus: Percentage of firms investing in this type of fraud prevention in the next year:
IP protection (32%)



medication online. In order to address the risks inherent in such purchases, Mexico's Federal Commission for Protection Against Health Risks banned all online pharmacies, including legitimate ones.

Theft

Drug theft, estimated to have cost companies \$235 million in Mexico in 2008, remains the leading risk in the minds of executives especially as, beyond the direct losses, it provides the counterfeit market with raw material and packaging. The problem comes in three primary forms: cargo theft, break-ins, and pilferage.

Pharmaceutical cargo is an attractive target for organized crime. The latter can exploit vulnerabilities throughout the distribution network. High value, quick marketability, ease of rechanneling, and relatively small penalties if caught make this kind of theft good business for criminals. Insurance companies estimate that every month one percent of all cargo trucks on Mexican roads are attacked, and Kroll puts the loss to the pharmaceutical industry in 2008 from this activity at \$80 million.

Gangs often have accomplices within distribution and transport companies who help identify targeted drugs, as well as provide shipping information and truck itineraries. Kroll has found that, in over 80 percent of thefts, a company employee is directly involved. Jalisco, Mexico State, Guanajuato, Mexico Distrito Federal, and Michoacán see 65 percent of all these crimes, largely because these same states serve as distribution and command centers for organized crime.

While cargo theft can affect all players, break-ins mainly target warehouses and retail drug stores. According to the National Association of Pharmacies, every pharmacy in Mexico experiences theft on average twice a year. Countrywide, this results in over forty thousand break-ins annually, and estimated losses of \$62 million.

Pilferage, on the other hand, usually takes place further down the distribution network and is particularly rampant within government institutions. Although there are no official figures, Kroll estimates that losses in Mexico are approximately \$93 million per year.

In seeking drugs, whatever the means, organized crime commonly focuses on medication of which the sale is restricted in the open market – such as psychotropic drugs – or on products with high market demand – such as lifestyle medicines. On the black market, these drugs are less expensive and easier to obtain, with no prescription required.

Sale of medical samples

The commercialization of medical samples hurts companies in two ways: first as an unprofitable use of resources in producing them, and second as a missed sales opportunity. It is calculated that the practice represents a lost market opportunity of \$90 million per year.

With drug sample production taking up between one and eight percent of pharmaceutical manufacturing capacity, some 20 million units are produced each year. Sales reps and doctors then sell the samples to “specialized collectors.” These, in turn, channel the products onto the black market, reaching clients mainly through street markets, irregular pharmacies, and online sales.

Looking forward

Pharmaceutical companies operating in Mexico are realizing that the risks outlined here erode their market position and long term competitiveness. It is no longer possible to dismiss the problem as simply a cost which companies have to endure. The long term profitability of manufacturers and distributors requires the implementation of preventive measures and anti-counterfeiting technologies, such as monitoring systems and authentication methods.

Technology, however, is not enough. Pharmaceutical companies are now acknowledging that good distribution channel management – that prevents the infiltration of counterfeit medication and stops the detour of products into illegitimate channels – is just as important.

Above all, most companies agree that they cannot tackle these problems alone. Whether partnering with law enforcement authorities to avert cargo theft, or with other companies to lobby the government on anti-counterfeiting laws, leading industry players are becoming more proactive in understanding and mitigating the substantial fraud risks which they face.

Guillaume Corpart is an associate managing director and expert in the field of market intelligence in Latin America. He joined Kroll in 2008 following the integration of InfoAmericas, the leading independent market intelligence firm in Latin America. He is a strategic advisor to clients, providing advice on market positioning, market entry, competitive trends, and partnering.

Manuela D'Andrea is an analyst in market intelligence in Latin America. She joined Kroll in 2008 following the integration of InfoAmericas. Manuela is responsible for primary and secondary research about market positioning, market penetration, competitive trends and associations.

Enrique Orellana was until recently a senior analyst within Kroll's market intelligence division, focusing on political and market analysis. He is now studying International Policy Management at Georgetown University.

EIU SURVEY

Lower incidence, higher costs: The health, pharmaceuticals and biotechnology sector has had some success in reducing the incidence of fraud, but the level of crime still taking place is costing more and keeping executives worried about their level of vulnerability.

- For eight out of ten categories of fraud covered in the survey, the proportion of sector companies affected over the last three years was less than that of the 2008 survey. Some of these declines were particularly notable. The proportion involved in regulatory or compliance breaches dropped from 37% to 22%; that for vendor, supplier or procurement fraud from 24% to 10%; and for corruption and bribery from 20% to 10%. The results for the last two categories were the best of any sector. Management conflict of interest was the most widespread problem in the industry rising from 28% to 31%.
- At the same time, however, the average loss per company over the last three years was \$11.7 million, or 133% of the overall average. This represented a substantial increase from the 2008 levels of \$7.8 million and 94%, although is more a return to the 2007 figures of \$11.7 million and 175%.
- Accordingly, more companies than average considered themselves highly vulnerable to eight out of ten categories of fraud covered in the survey.
- In particular, despite having fewer companies suffer from information loss than in the survey as a whole (21% compared with 25%), 27% of sector companies rated themselves highly vulnerable to information theft, the highest figure of any industry. Similarly, the number considering themselves highly vulnerable to IP theft, at 24%, was the highest of any sector, yet the number of healthcare, pharmaceuticals and biotech companies hit by this type of fraud was only slightly above average (16% compared with 14%).

Little change in spending: These concerns are having an uneven impact on spending priorities.

- Sector companies are slightly more likely than average to have in place IT security measures (74% compared with 71%), and noticeably more likely to have IP monitoring (47% compared with 36%).
- More sector firms than in any other industry plan to invest in IP protection in the coming year (32%), but only an average number will do so for management controls (34% for the industry and for all sectors combined).

Healthcare, pharmaceuticals and biotechnology companies have been successful in keeping down the prevalence of fraud and, in particular, the number of IT attacks and incidents of IP theft, in an industry where both can have a devastating impact. Their continued efforts should help to bring down the cost of fraud, but executives should now consider how to address the problem of management conflict of interest more effectively.

Written by The Economist Intelligence Unit

EIU SURVEY

Fraud levels are relatively low: The technology, media and telecommunications sector performed well last year compared to its peers.

- It had the third-lowest average loss per company, \$4.7 million, or 54% of the overall average. Although this is partly the result of an unusually high number of smaller companies in the industry, the figure is still low.
- The sector had the lowest prevalence of fraud, with just 73% of companies hit in some way in the last three years.
- For eight out of ten categories of fraud, the percentage of companies falling victim in the last three years was below the survey average.
- Moreover, fewer industry firms suffered from internal financial fraud (8%) than any other sector, and it came in second best on theft of physical assets (29%).

Threats remain: IT and IP theft mar an otherwise good performance, but also of concern is a tendency not to look beyond these risks.

- The two obvious threats to the industry are information theft and IP theft. In the last three years, 29% suffered from the former – the highest sector figure – and 16% from the latter.
- Companies defend themselves accordingly. The sector has the most widespread deployment of IT security (in place for 83% of companies) as well as above average use of IP monitoring (41% compared with an average of 36%). In both cases, more technology, IT and media companies than average are also looking to invest in these areas in the coming year. In previous years, concern about these issues seemed very high compared to their actual incidence, but now the two seem more aligned.
- By contrast, in the coming year, fewer sector companies will be investing in every other anti-fraud strategy listed
- This may be justifiable in some cases, given the low incidence of many types of fraud, but the sector suffers from the same rate of financial mismanagement as the overall survey average (21% of companies over the last three years), yet notably fewer firms have financial controls in place (69% compared with 82%), and fewer also plan to invest in this area (39% compared with 46%).

Fraudsters are nothing if not inventive, and even industries that are achieving good results will need to be vigilant in the face of new challenges – 31% of sector companies, for example, say that the downturn has increased the incidence of fraud. Technology, media and telecommunications companies might therefore improve on this relative success by looking beyond the obvious fraud risks, while continuing their efforts against IT attack and IP theft.

Written by The Economist Intelligence Unit



IT outsourcing: Is it worth the risk?

Paulo R. Silva

IT outsourcing has long been an accepted solution for companies to streamline processes, reduce costs, and provide flexibility to meet the changing demands of their operations. With the global economic crisis forcing business leaders to squeeze out additional operational efficiencies to survive, more outsourcing seems inevitable. The decision, however, on what functions to outsource is often made without a thorough assessment of the risks involved in determining what is to be outsourced, and to whom.

In January 2009, India's Satyam Computer Services, then the fourth largest outsourcing company in the world, shook the sector by admitting that it had systematically inflated revenue and profits for years. The corporation was eventually sold to another Indian firm, Tech Mahindra, to restore confidence in the market and ensure the continuity of its operations.

Satyam's fraud and lack of internal integrity should serve as a wakeup call for companies intending to use IT outsourcing

services. The Satyam case presents a strong reminder that technology companies, including IT outsourcing ones, are vulnerable to the same common frauds – such as internal financial fraud, vendor or procurement fraud, and theft of physical assets – that can occur in any other business.

Moreover, even though IT outsourcing companies, as obvious targets, invest heavily to prevent cyber crime, they can also be victims of fraud typically related to the cyber world, such as information theft and intellectual property theft. 29 percent of IT, media, and telecommunication firms have suffered from the former in the last three years, and 16 percent from the latter, according to the 2009 Kroll Global Fraud Survey. The survey also shows that roughly a fifth of sector companies feel themselves highly vulnerable in these areas.

In February 2008, the Bank of New York Mellon was a victim of data breach while under the responsibility of an outsourced company. Unencrypted back-up tapes containing personal information of over 12 million customers disappeared during transport to an off-site facility. Although no misuse of information from the tapes was

REPORT CARD

TECHNOLOGY, MEDIA AND TELECOMS

Financial Loss: Average loss per company over past three years \$4.7 million (54% of average)

Prevalence: Companies suffering fraud loss over past three years 73%

Increase in Exposure: Companies where exposure to fraud has increased 81%

High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable to specific frauds
Information theft, loss or attack (21%) • IP theft, piracy or counterfeiting (19%)

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in last three years

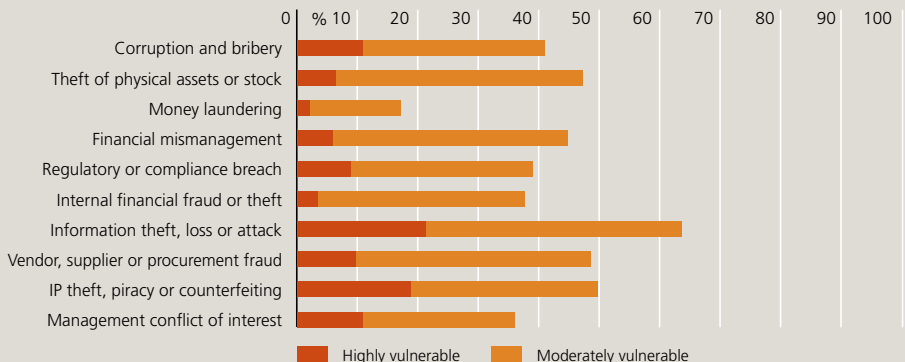
Theft of physical assets or stock (29%) • Information theft, loss or attack (29%)

Management conflict of interest (21%) • Financial mismanagement (21%)

Investment Focus: Percentage of firms investing in this type of fraud prevention in the next year:

IT security (59%) • Financial controls (39%) • Physical asset security (34%) • Management controls (33%)

IP and trademark monitoring program (31%)



identified, this incident caused large losses for the bank since it had to take actions such as internal investigations and assistance for those who had personal information stored in the back-up tapes. Such frauds frequently occur when companies presume that the IT outsourcing business, which they hired, has the same security procedures as their own. If custody of, or responsibility for, sensitive information is outsourced, the contracting company may be compromised in any subsequent security breach.

Other outsourced services are also subject to frauds. Companies must, therefore, strategically and cautiously decide what will be outsourced, and then carefully select which company will get the contract. Here are some factors that should be considered:

Determine what should or should not be outsourced: Many companies outsource activities which are not related to their core business, such as management of their IT infrastructure, in order to gain competitive advantage through streamlined processes, increased flexibility, and reduced costs. Companies must be careful when passing crucial information or processes to third parties; the sharing of such information brings information security risks.

Select the appropriate services provider: Consider the capacity of the supplier to handle the volume of services required. Conduct a pre-screening investigation based not only on suppliers' credentials but also on a thorough understanding of the services offered. Supplier benchmarking is an effective way to weigh provider options.

Consider multisourcing: This model can increase flexibility and reduce risks in the outsourcing project. And, while it does demand greater effort to manage contracts with several suppliers, the selection of choosing a single supplier – full outsourcing – requires more careful selection processes, since that firm will share more heavily in the risks of the company.

Outsourcing can provide great benefits, but it may cause problems when the company loses direct control over the management of outsourced services. The Satyam incident warns us of the risks run when we put all our eggs into the same basket.



Paulo Renato Silva is an associate director in Kroll's São Paulo office. He specializes in information security and has coordinated many projects in the computer forensic field in Brazil as well as across Latin America. He has a Bachelor's Degree in Computer Science from the University of the State of São Paulo, and is a member of the Information Systems Security Association.

The Foreign Corrupt Practices Act, the Siemens settlement, and the energy sector



David A. Holley

The energy industry has long been fertile ground for corruption and bribery and, therefore, ripe for Foreign Corrupt Practices Act (FCPA) enforcement activity. By its very nature, the international energy business, including the oil and gas sector, requires a high degree of government involvement and cooperation, particularly when entering markets overseas, constructing facilities in new territories, applying for permits from foreign agencies, or reaching distribution agreements with countries. Such cooperation can be achieved in many ways, and some firms resort to methods with FCPA implications.

The most recent example of an energy company undergoing an FCPA investigation and prosecution ended in a December 2008 settlement between Siemens AG, the United States Department of Justice (DOJ), and the Securities and Exchange Commission (SEC). The case provides lessons for every international energy firm on how to remain FCPA compliant as it develops business and establishes a presence overseas.

Cooperation with Government investigations: Siemens' approach to the FCPA investigation has been universally recognized as the "right way" and can serve as a model for those facing similar actions. Siemens retained a multi-national team of accountants and lawyers to establish

the facts and circumstances surrounding all of the allegations. The company was also reportedly timely and forthcoming with all of the DOJ's requests for documents and information. The settlement agreement calls Siemens' level of cooperation "exceptional." This behavior is said to be why the company secured the terms it did. Approaching an FCPA investigation cooperatively, rather than contentiously, is the single greatest lesson coming from the case.

Due diligence failures: Siemens' failure to perform meaningful due diligence on some third-party consultants led to many of its FCPA-related problems. Numerous "red flags" relating to their hiring and use went mostly undetected because of a failure to centralize the due diligence and third-party retention processes. For example, Siemens engaged certain consultants with no relevant experience in their contracted tasks and many received unusually high fees relative to the going rate for such work. In addition, the company used third parties concurrently employed by the governments with which it was seeking a business relationship. Engagement of a third party should always be preceded by a level of due diligence which will yield full knowledge of its proposed activities, remuneration, and expertise to carry out its mission.

Management's role in compliance: Siemens was harshly taken to task for management's apparent failure to ensure FCPA compliance in parts of its overseas business. The SEC complaint criticized Siemens' FCPA compliance program, saying

bribe payments and inadequate controls were "accepted by senior management." The DOJ admonished Siemens' senior leadership for failing to instill ethics into its business by, for example, not making a clear statement of company policy to employees on the payment of bribes. In essence, the government was condemning a failure of corporate leadership to create a "tone at the top" consistent with effective compliance. Management buy-in involves more than just promulgation of FCPA-related rules: senior executives must be actively engaged to ensure not merely conformity with the letter of the law, but also an ethos of compliance.

The Siemens case provides numerous FCPA compliance lessons for the energy industry. As expansion in foreign markets makes contracting with unfamiliar governments inevitable, energy concerns will sometimes face unfamiliar cultural expectations and challenges. Meeting these ethically and legally will certainly test even the most compliant entities. In these efforts, the Siemens case can provide some guidance and may even become an example for regulators in future enforcement activities.



David A. Holley is a senior managing director and the head of Kroll's Boston office. Since joining Kroll in 2000, David has led investigations including environmental matters, contests for corporate control, internal investigations and white-collar crime investigations. Prior to joining Kroll, David worked for a mid-sized investigative firm and the Environmental Enforcement Section of the US Department of Justice.

EIU SURVEY

Fraud levels: The latest survey contained both positive and negative results on the incidence of fraud levels among natural resources companies.

- On the positive side, the average loss to fraud over the last three years, at \$8.0 million, was less than one-half of the amount from the 2008 survey, at \$18.1 million. Moreover, even though natural resources companies are larger as a group than those in other surveyed sectors, the industry's average loss this year was below that for the whole survey (92%).
- In addition, only 13% of industry companies report an increase in fraud levels during the last year, compared with 32% which cite a decline. Both of these improvements probably reflect the global decline in exploration and investment in oil, gas and mining in the last 12 months.
- On the negative side, 52% of sector companies suffered from theft of physical assets in the last three years, the greatest proportion hit by any fraud in any sector. Moreover, one in four experienced each of information theft, vendor or procurement fraud, and corruption or bribery – in the last case this was the second-highest figure of any sector.
- Overall 93% of natural resources companies were hit by some sort of fraud in the last three years, the highest proportion of any sector, although not a significant change from last year's survey.

Consistent spending: The problem is not one of insufficient attention.

- Of the ten categories of anti-fraud measures covered in the survey, nine were more widespread among natural resources firms than on average. For staff screening, the only exception, the difference was just 1%.
- Two of these measures were more widely deployed in this sector than anywhere else: staff training (59% use it compared with 45% on average); and partner, client and vendor due diligence (57% compared with 46%).
- Just 7% had weakened internal controls as a cost-saving measure, the second-lowest result in the survey.

Inherent fraud risks: Instead, the sector's perennial problem is exacerbating fraud risk – the need to go wherever the raw materials are, however problematic the operating environment. Entry into new, riskier markets had increased fraud vulnerability for 38% of natural resources firms, making it the sector most affected by this issue.

This year's results present a mixed picture for natural resources – one of a sector with serious fraud risks that it is working to address, with some success.

Written by The Economist Intelligence Unit

REPORT CARD NATURAL RESOURCES

Financial Loss: Average loss per company over past three years \$8.0 million (92% of average)

Prevalence: Companies suffering fraud loss over past three years 93%

Increase in Exposure: Companies where exposure to fraud has increased 79%

High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable to specific frauds
Corruption and bribery (23%) • Information theft, loss or attack (21%) • Theft of physical assets or stock (21%)

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in last three years

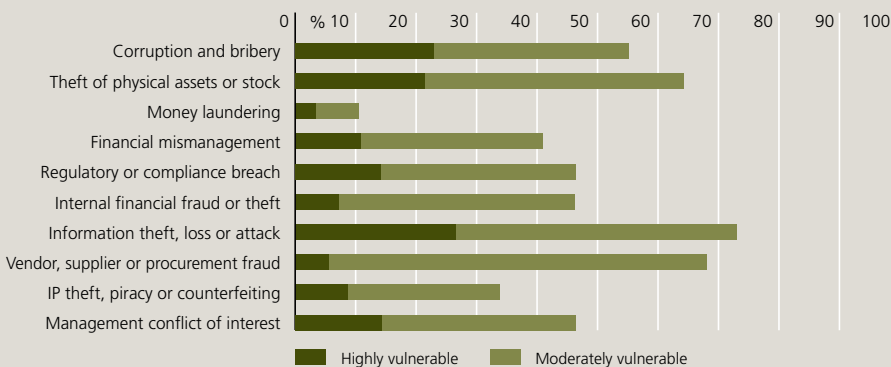
Theft of physical assets or stock (52%) • Information theft, loss or attack (27%)

Vendor, supplier or procurement fraud (25%) • Corruption and bribery (25%)

Regulatory or compliance breach (20%)

Investment Focus: Percentage of firms investing in this type of fraud prevention in the next year

IT security (50%) • Financial controls (39%) • Management controls (32%) • Staff training (32%)



MIDDLE EAST & AFRICA OVERVIEW

It is difficult, at first glance, to see anything positive in the fraud survey figures from the Middle East and Africa. Once again the region is by far the worst affected.

- For seven out of ten frauds covered in the survey – corruption and bribery (affecting 34% of regional respondents); vendor fraud (33%); management conflict of interest (31%); financial mismanagement (31%); internal financial fraud or theft (27%); IP theft (22%); and money laundering (12%) – the Middle East and Africa had the highest incidence of any region. The number of companies hit by the remaining three frauds was, in each case, also above average.
- For five out of ten frauds, the region also has the most companies considering themselves highly vulnerable: corruption and bribery (27%); vendor fraud (22%); theft of physical assets (17%); IP theft (16%); and financial mismanagement (14%).
- The Middle East and Africa saw the most companies whose vulnerability increased due to high staff turnover (36%); weaker internal controls to save money (27%); pay restraint resulting from reduced income (21%), and reduced revenue in general (16%).
- The average loss per company over the last three years more than doubled from the 2008 survey figure, from \$5.6 million to \$11.5 million, although this came as a result of an increase in the number of respondents with losses over \$100 million rather than as a result of an across the board shift upward.

On the other hand, last year's survey figures were in some respects even worse, and companies are taking steps to address the problem.

- Of the ten categories of fraud, three were more prevalent among survey respondents this year, including notably vendor fraud which rose in incidence from 24% to 33%. Three, however, stayed roughly the same, and four actually dropped. The latter included last year's two most widespread frauds: theft of physical assets (down from 46% to 38%), and management conflict of interest (from 43% to 31%).

- 36% of respondents saw a drop in fraud at their companies, against 28% who observed an increase.
- The number of firms reporting increased vulnerability to fraud as a result of high staff turnover and weaker internal controls was also down.
- With the exception of IP protection measures, a greater proportion of regional companies than average will be

investing in every anti-fraud strategy listed in the survey, including notably IT security (58% of regional companies compared with 51% on average), and physical asset security (56% to 37%).

It would be wrong to characterize the fraud situation in this region as anything but extremely serious. It is, however, fair to note some improvements. Moreover, companies certainly have not given up.

	2009	2008
Financial Loss: Average loss per company over last three years	\$11.5 million (147% of average)	\$5.6 million (68% of average)
Prevalence: Companies suffering fraud loss over last three years	88%	91%
High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable	Corruption and bribery (27%) Vendor, supplier or procurement fraud (22%)	IP theft, piracy or counterfeiting (24%) Information theft, loss or attack (23%) Management conflict of interest (22%) Corruption and bribery (21%)
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in last three years	Theft of physical assets or stock (38%) Corruption and bribery (34%) Vendor, supplier or procurement fraud (33%) Management conflict of interest (31%) Financial mismanagement (31%) Internal financial fraud or theft (27%) Information theft, loss or attack (26%) Regulatory or compliance breach (23%) IP theft, piracy or counterfeiting (22%)	Theft of physical assets or stock (46%) Management conflict of interest (43%) Financial mismanagement (38%) Corruption and bribery (34%) Information theft, loss or attack (29%) Internal financial fraud or theft (27%) Vendor, supplier or procurement fraud (24%) Regulatory or compliance breach (23%)

Spotlight on Nigeria

Fraud incidence in Nigeria broadly mirrors that in the region as a whole. The two biggest exceptions are: money laundering, which affected 19% of Nigerian respondents in the last three years compared to 12% across the region and just 5% of the whole survey; and IP theft (30%, compared to 22% and 14% respectively). Although Nigerian companies are more likely than those in

their region or globally to feel highly vulnerable to both frauds, they are tackling money laundering more actively than IP theft.

Some 93% of companies in the country have financial controls in place (compared with 82% globally), but only 30% of Nigerian respondents have IP protection measures in place (compared with 36% worldwide). As IP theft, piracy, and counterfeiting are rising in the Middle East and Africa, this could make them even more vulnerable than they are now.

India's retail sector: Risks that match the potential rewards



REPORT CARD RETAIL, WHOLESALE AND DISTRIBUTION

Financial Loss: Average loss per company over past three years \$12.7 million (145% of average)

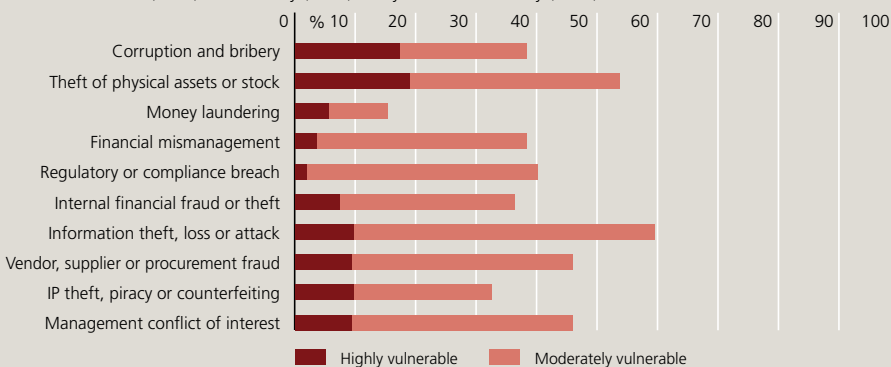
Prevalence: Companies suffering fraud loss over past three years 92%

Increase in Exposure: Companies where exposure to fraud has increased 71%

High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable to specific frauds
Theft of physical assets or stock (19%) • Corruption and bribery (17%)

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in last three years
Theft of physical assets or stock (42%) • Vendor, supplier or procurement fraud (27%)
IP theft, piracy or counterfeiting (21%)

Investment Focus: Percentage of firms investing in this type of fraud prevention in the next year
Financial controls (44%) • IT security (40%) • Physical asset security (37%)



Richard Dailly

For years rumors in the retail industry have predicted the imminent, complete opening of the Indian retail sector to non-Indian operators. Since the economic liberalization measures of 1990 were legislated, the amount of foreign direct investment (FDI) flowing into this sector, together with many others, such as banking, insurance, and print media, has been closely controlled by the Indian government. Partly as a result, India's retail sector remains highly fragmented: 97 percent of the market belongs to unorganized outlets; just three percent to organized ones. India's retail sector remains one of the few large unconsolidated markets in the world.

Change will not happen overnight. Echoing various previous statements of Indian policy makers, on August 15, 2009, India's minister of state for commerce and industry, the governor of its central bank – the Reserve Bank of India – and the head of

the government's economic advisory council unanimously stated that there was "no proposal to implement full capital account convertibility." Full capital account convertibility allows long term investors to repatriate all their profits, whereas partial capital account convertibility requires them to reinvest in the business a significant part of their profits. This ensures that a large part of foreign investment stays within India. Such a step strikes Indian policymakers as extreme towards opening up Indian markets.

Nevertheless, it is widely believed that the government is committed to increasing the amount of FDI in the retail sector, albeit incrementally. The government believes that the absorption of investment into the retail sector needs to be slow, in order not to dislocate existing family-run stores, but rather to create jobs for the children of these merchants. For the government, it is not a question of FDI versus no FDI; it is a question of big against small.

Investors bold enough to be first movers face daunting operational risks in an immature market including an inefficient and corrupted supply chain and logistics industry upon which it relies. Abundant but poorly written and enforced industry standards are cumbersome to comply with, dragging on efficiency. Suppliers are fragmented and susceptible to counterfeit product, stock-outs, and quality inconsistencies.

One of the leading threats to retailers, of both Indian and mixed capital, is shrinkage. In more mature markets, shrinkage typically ranges from 1-2% of Cost of Goods Sold (COGS). In India, the metric is estimated to be much higher. Supply chains are not at the mercy of the inherent weaknesses of India's infrastructure and distribution networks. They are also vulnerable to the officials who oversee infrastructure operations and to any other individual with whom goods come into contact. An example of this is the practice of transport companies that are hired because they have family links to the key official who controls the state border crossings. Kroll investigated one company who used this tactic to dramatically reduce the transit time from the south of India to Delhi – from three days to one and a half. Other sources of shrinkage include: short-weighting, pilferage, insecure vehicles, and poor product handling, all producing losses to be covered by the retailer.

Tracing shrinkage is an enormous challenge. Given that most transactions are still handled on paper-based systems, the audit trail for the movement of goods is often impossible to follow. Large retailers reveal that they have not been able to achieve any more success than their smaller competitors when it comes to combating shrinkage.

An important source of shrinkage originates from within the retailer, i.e. its employees. Amid widespread poverty, significant loyalty to a faceless corporation of apparently limitless wealth is unlikely. Countering this demographic reality are good practices that large retailers can employ such as background checks on all levels of staff and the construction of a strong, identifiable and magnanimous business culture.

Despite India's reputation for churning out high caliber professionals, there is a shortage of managerial talent at the top of the Indian retail sector. Stories abound of unprofessional management, even among some of the biggest names in the country, probably because many major Indian retailers began as family businesses. Like many family run companies around the world, the prize C-suite positions in Indian retailers are reserved for family members and close friends. The absence of meritocracy prevents the hiring of experienced managers or the promotion of able mid-managers. The lack of professionalism, mixed with family politics leads to under-performance and unsupervised fraud and waste. One un-named Indian retailer revealed that they had not measured stock in several years.

As with every other Indian sector, any new retailer must navigate the maze of regulatory interference. Regulations require upwards of 30 license approvals, and any license approval in India is subject to abuse. At the political level, local strong-arm parties frequently demand employment for members. Large retailers entering the market would be perceived as a significant threat to the traditional way of life in some areas. This, combined with populist, aggressive political leaders and strong unionization, could provoke physical risks to high profile investors and managers.

In a world of modern retail, India stands out as one of the last great investment opportunities. The first investors will be attracted by the seemingly limitless opportunities. However, the risks they face, whether they are be they political, sectoral, physical, labor, or regulatory in nature, are equally daunting. Market entry must be carefully planned with a steady flow of business intelligence feeding the business decision process.



Richard Dailly is a managing director in Mumbai. He has many years of experience working in international politics and political risk for the British government and Kroll. Richard has a deep understanding of investigative and intelligence techniques and analysis, in support of corporate investigations, due diligence, political risk and litigation support.

EIU SURVEY

The retail, wholesale and distribution sector has a serious fraud problem, of which it is insufficiently aware.

High levels: Fraud has risen to high levels.

- Although companies in this sector, as a group, are smaller than average, the loss to fraud per company in the last three years was \$12.7 million or 145% of the norm. This exceeded the overall average for the first time since these surveys began, and was also dramatically greater than the 2008 figure of \$3.3 million.

- A total of 92% of sector companies were affected by fraud, the second-highest rate in the survey.

The increased incidence of fraud seems to have appeared suddenly in the last year. When asked about ten specific types of fraud suffered over the last three years, respondents reported lower figures for seven of these, sometimes noticeably. Those affected by theft of physical assets in the last three years, for example, dropped from 67% to 42%.

On the other hand, when asked in a separate question about fraud in the last twelve months, for two categories this sector was more affected than any other – theft of stock and financial mismanagement – and for four more it performed second worst – internal financial fraud, corruption and bribery, IP theft, and money laundering.

Insufficient attention: Perhaps because the upswing appears to be recent, the sector as a whole seems to be giving the issue less attention than its peers.

- Despite its high level of fraud prevalence, a below average number of sector companies deploy every anti-fraud measure covered in the survey.

- Spending on nine out of ten of these measures is also predicted to be less widespread in this sector than for the survey as a whole, with only 8%, for example, spending to bolster IP security – less than the number affected by IP theft, and about one-third of the survey average (23%).

The retail, wholesale and distribution sector needs to act to address the recent uptick in fraud. Otherwise, levels of fraud risk may only increase.

Written by The Economist Intelligence Unit

Multiple-source reporting: What works for tax fraud could work for Ponzi schemes

Using IRS-type reporting mechanisms, Ponzi schemes such as Madoff's could have been uncovered sooner, says Dr. Marcia Kramer Mayer.

How does \$65 billion in assets purportedly under management go missing? That was the sum of the account values that Bernard Madoff Investment Securities (BMIS) reported to clients throughout North America, Europe, and Latin America on their November 2008 statements. Virtually none was real, as the world learned days later when the biggest-ever Ponzi scheme came to light. Some 5,000 direct investors and untold thousands with money in feeder funds saw their supposed net worth collapse in an instant.

An exhaustive report issued on 31 August 2009 by the SEC Office of the Inspector General (OIG) tells the story of how the SEC was fooled by Madoff's machinations despite the creditable and detailed complaints and significant red flags that whistleblowers and journalists brought to its attention as early as 1992, and the two investigations and three examinations that ensued. The OIG report rules out inappropriate connections or influence as factors in the bungled investigation. Rather it finds the problem to have been inexperience and financially naive staff, misplaced priorities, internal communication failures, and lack of appropriate follow-up and the repeated failure to seek third-party corroboration of Madoff's claims.

Clearly, we need a better way. From the standpoint of early monitoring rather than probable-cause investigation, the current regulatory regime for investor advisor fraud detection falls short on four counts.

First, most investment advisors are not required to register with the SEC. Some are exempt because they manage less than \$25 million, but a significant number are exempt because they have fewer than 15 clients, as each hedge fund advisee counts as just one client for registration purposes.

Second, SEC registration is not a game-ender for Ponzi operators. Madoff was registered but lied in his disclosures. On his last Form ADV, filed January 7, 2008, he reported \$17 billion in assets under management: far below the \$65 billion he told investors later that year – even though markets had crashed in the interim – but higher than the negligible amount he actually held on their behalf. Another huge falsehood was his reported client count: 23, versus the 4,903 active accounts that administrators found upon the firm's demise. The SEC simply has no ready way to validate the representations of registered investment advisors or even to know when they are giving contradictory stories to customers and regulators.

Third, the current system has no requirement for investment advisors to use an independent custodian. BMIS truthfully disclosed that it did not do so. By permitting advisors to provide self-custody, current law facilitates misrepresentations about assets under management. The danger is compounded if the advisor uses a captive, no-name auditor, as did BMIS.

Finally, in the current system oversight is resource-intensive. Large numbers of financially sophisticated inspectors would be needed to conduct routine, comprehensive reviews competently. Budget constraints preclude such an approach.

Two proposals of note try to address the problem. The Obama Administration's regulatory reform bill would require hedge fund advisors to register with the SEC if they managed at least \$30 million in assets. A pending SEC proposal would effectively mandate a qualified independent custodian. Both measures would help in Ponzi scheme detection, but they do not go far enough.

One concern about the SEC plan is that a supposedly independent custodian might be complicit with a scheming advisor. Another is that a Ponzi artist might direct substantial incoming customer assets in such a way that the custodian never learned of them, and so could not see them getting siphoned off.

As for the Administration bill, investment advisors to funds are covered but those with discretion over non-pooled monies are not. Madoff did not operate a hedge fund;

he purported to invest on behalf of clients individually. Another weakness is that the bill gives the SEC no means to test the veracity of a registrant's disclosures. If a custodian were complicit with or deceived by an advisor client, the task of asset validation would fall to the SEC.

The law should better equip the agency to perform its investigations. If Congress and the SEC are serious about protecting investors from Ponzi schemes, they need look no further than the Internal Revenue Service (IRS) for an approach that is both simple and well tested: multiple-source reporting of entity-specific data. Rather than accept at face value the income components that taxpayers report on their personal tax returns, the IRS comprehensively cross-checks those claims against statements of wages, interest, dividends, and gross sale proceeds submitted by employers, financial institutions, and other income payers. It then attempts to reconcile any identified discrepancies. Routine cross-checking improves the accuracy of the final numbers not only by correcting errors but also by motivating honest reporting in the first place.

The SEC must be similarly empowered to routinely and cost-effectively validate the data that it needs to police investment advisors. Instead of having it rely exclusively on the most self-interested party – the advisor – for routine information on assets under management, a system under which multiple organizations would be required, and

individual investors encouraged, to provide the SEC with data about each advisor's managed assets, would be preferable.

Investment advisors with at least \$30 million under management would be required to report quarter-end assets by account – identified by code, not name.

Custodians would have to report quarter-end assets under management for each advisor-client. To give teeth to this mandate, advisors would be required to use an independent custodian.

Investors would be invited – but not required – to report quarter-end assets under management by advisor and account.

This data would be fed into software that made comprehensive comparisons efficiently, checking whether the total assets under management per an advisor's aggregate reported account-level assets matched the overall sum given by the custodian, and whether account-level assets as per the advisor agreed with those reported by participating investors.

For any given date and level of aggregation, the values should agree. If there were large, numerous, or recurrent discrepancies for an advisor, a well-focused SEC inquiry could be launched to determine whether any claimed assets were missing.

The involvement of individual investors is the linchpin of this plan. Even with a truly independent custodian, an advisor could run a Ponzi scheme by having some investment monies deposited into accounts of which the custodian was unaware, while the firm ran a legitimate operation with

assets that the custodian did see. An advisor engaged in such asset diversion would report to the SEC only those assets under management to which its custodian was privy. If the SEC had no ready means of learning that the advisor was reporting larger numbers to investors, the scheme might go undetected. An asset-diverting advisor, however, would have no protection under this plan from random investors reporting their individual account asset values. Unless the advisor informed the SEC of all account-level assets, any one investor report could trip it up.

In the end, Ponzi scheme prevention and detection requires keeping an eye on customer assets. If investor self-interest can be harnessed to motivate at least some advisory clients to report their assets under management. And if advisors can be made to fund the system, securities regulators who adopt a multiple-source reporting system such as the one proposed here can tackle the Ponzi problem quickly, effectively, and at minimal cost to tax payers.



Dr. Marcia Kramer Mayer is a senior vice president of NERA Economic Consulting, where she directs projects in the areas of securities and finance. She has examined issues of market efficiency, class certification, liability, materiality, damages, settlement

prediction, and claiming rates in hundreds of shareholder class actions. Dr. Mayer came to NERA from the American Stock Exchange, where she was a Vice President. In her prior academic career, Dr. Mayer was a Lecturer in the Department of Community Medicine at the State University of New York at Stony Brook and an Instructor at Swarthmore College. She holds a Ph.D in economics from Harvard University.

Chinese fakes in Kor



Nicholas Blank

The global apparel market is predicted to reach nearly \$1,800 billion by 2011.¹ Globalization has shifted production toward developing countries, especially China. That country's National Garment Association estimates Chinese production capacity at 52 billion pieces per year. The country's 120,000 manufacturers give United States and European fashion companies a wide variety of potential suppliers. Along with the benefits of increased competition, however, a dark side has emerged: counterfeit apparel.

¹ <http://www.fashionproducts.com/fashion-apparel-overview.html>

Anyone traveling to Asia can find illegal imitations simply by walking through local marketplaces. With vendors and hidden showrooms spread through mazes of alleys, these places attract tourists on buying sprees for cheap designer fashions. Some counterfeit garments are outright unlicensed copies; others are made by authorized manufacturers that fail to prevent rejects from "going out the backdoor."

China is struggling to clean up. According to Kroll's Global Fraud Survey, nearly a quarter of companies in this region have experienced IP theft in the last three years. The country is on the United States Trade Representative's (USTR) Special 301 Priority Watch List and has two marketplaces on

the Notorious Markets List. For the first time, however, South Korea is not on even the USTR Watch List, and neither Dongdaemun nor nearby Namdaemun Markets are listed as notorious markets.

Despite Seoul's persistent intellectual property rights efforts, major problems remain. Recently Korean Customs, for example, acted against an online dealer who sold, over two years, 70 thousand counterfeit luxury items worth \$1.26 million. The dealer procured his stock from Namdaemun Market. Another counterfeiting operation sold 10,000 pairs of grade 'A' copies of shoes at Dongdaemun and Namdaemun Markets.

Asian markets

Many of Korea's counterfeits originate in China. Guangzhou is a key location for procuring fakes to ship back to Seoul. Several years ago, working with the local Administration of Industry and Commerce (AIC), Kroll organized raids against stalls in Guangzhou's Wan Tong garment market. Several times, Korean nationals arrived on the scene during the raid. Unable to speak Mandarin, they would argue with AIC officers through translators. One Korean, wearing dark sunglasses, demanded to see the AIC officers' badge; another became physically aggressive. Clearly the raids were disrupting a profitable trade route.

Traditionally Koreans have a stronger presence in Northern China. Investigations around Qingdao indicate Korean involvement in counterfeiting there. During our investigations in the region, Kroll also found smuggling routes from Northern China into South Korea, with smugglers posing as passengers on ferries from Dalian to Incheon. Cargo agents, based in a cheap hotel near Dalian, often help with visas and shipping arrangements. The Korean Customs Service, in a crackdown from January to May 2009, dealt with 186 cases from China.

To learn more about the origins of fake apparel in Korea, we surveyed vendors at Namdaemun and Dongdaemun Markets. They almost all denied that their garments

were Chinese-made. As proof of local origin, they said that orders could be delivered to their stalls in two to three days. Yet none gave further details about their factories in Korea. It seemed plausible that their garments were actually imported from China.

One vendor at Namdaemun, selling soccer uniforms, did admit that he bought them from a Chinese factory and then had them modified. It is easy to buy, or even custom order, "Made in Korea" tags and sew them onto imported garments.

Corporate brand protection efforts to address these issues can include, among other things, training programs for officials to familiarize them with English language brand names; garment tracing from major distributors back to factories; review of all licensee relationships; and preventive measures, such as regular audits of OEM and in-house factories. An audit that prevents T-shirts and jeans from being lost "out the back door" in China could very well save time and money in Korea.



Nicholas Blank is an associate managing director and head of Kroll's Seoul office. Nick is fluent in Mandarin and has over ten years of experience working in China.

EIU SURVEY

Above average results: The efforts made by the consumer goods sector to reduce levels of fraud are above average compared with other industries, and the economic downturn is not having an undue impact on fraud incidence.

- Consumer goods companies suffered below average financial damage from fraud, with the typical firm losing only \$2.8 million, or 31% of the survey average in the last three years, the lowest amount for any sector. The 2008 survey yielded a much higher figure for the preceding three years of \$12.7 million. The fall may be exaggerated, as last year's figure is also far out of line with that of 2007 – \$0.7 million – suggesting a statistical blip. Nevertheless, there was clearly movement in the right direction.
- Only 13% of industry respondents believe that the global economic crisis has led to a deterioration in the overall incidence of fraud, compared with 30% for the survey as a whole. Moreover, just 13% again say that they have seen a rise in fraud in the last year, compared with 32% who have seen a decrease.
- The percentage of companies that report being hit by fraud in the previous three years has decreased from the last survey for seven out of ten categories covered, sometimes substantially. For example, 22% report suffering from information theft, down from 32%, and 13% had experienced IT theft according to this year's figures, down from 30%.

Weak points: Small-scale fraud is widespread, and the industry has two particular weak points: loss of physical assets; and vendor, supplier or procurement fraud.

- Overall, 87% of sector companies experienced fraud in the last three years, little changed from the 2008 survey figure of 88%.
- Physical security is the sector's most widespread problem, and one that companies need to afford more attention.
- 48% of consumer goods firms have suffered from theft of physical assets in the last three years.
- Only 9%, however, consider themselves highly susceptible to this type of fraud

Moreover, although 83% of consumer goods companies have physical asset security measures in place – the best figure of any industry – in the near future only 30% expect to bolster these measures. The latter figure is less than the survey average (37%), even though losses in this area are far more frequent in this sector than elsewhere.

- 35% of sector respondents have suffered from vendor, supplier or procurement fraud in the last three years, compared with 20% overall.
- Fewer consumer goods companies than average have client and vendor due diligence measures in place (41% compared with 46%), and investment in such protection is also likely to be less widespread than average over the next year.

The threat of fraud is less severe for consumer goods firms than for those in many other sectors, and the financial losses are the lowest. Nevertheless, fraud remains a widespread problem, and two particular areas – theft and vendor fraud – merit greater attention.

Written by The Economist Intelligence Unit

REPORT CARD CONSUMER GOODS

Financial Loss: Average loss per company over past three years \$2.8 million (31% of average)

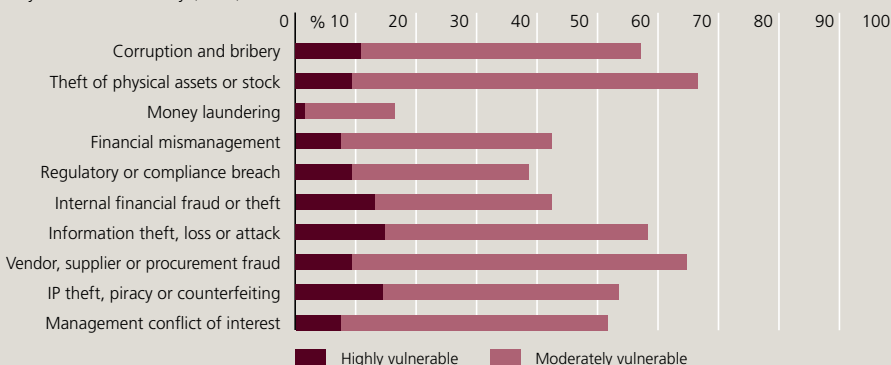
Prevalence: Companies suffering fraud loss over past three years 87%

Increase in Exposure: Companies where exposure to fraud has increased 68%

High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable to specific frauds
Information theft, loss or attack (15%) • IP theft, piracy or counterfeiting (15%)

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in last three years
Theft of physical assets or stock (48%) • Vendor, supplier or procurement fraud (35%)
Management conflict of interest (26%) • Information theft, loss or attack (22%)
Regulatory or compliance breach (20%) • Corruption and bribery (20%)

Investment Focus: Percentage of firms investing in this type of fraud prevention in the next year
IT security (47%) • Financial controls (44%) • Staff training (37%) • Management controls (33%)
Physical assets security (30%)





Fraud risks in commercial aviation

Vander Giordano

The aviation sector is among the most exposed to the world economic crisis. Operational costs are high and margins very low. Exchange rate fluctuations in countries with unstable currencies, for example, or fuel price volatility can lead to increased debt or poor economic performance. Financial risks can also come from non-economic factors: air disasters, even when a company's own planes are not involved, can bring an immediate fall in every airline's seat sales, impacting the whole industry.

Fraud, too, is a danger in this sector. According to Kroll's recent Global Fraud Survey, the problem is increasing in the transportation and leisure industry. Moreover, economic and operational developments such as those noted above can make fraud more complex and harder to address. Aviation firms need well-thought-out management strategies with up-to-date controls and continuous monitoring to prevent fraud wherever possible.

Here are some common situations and the related potential fraud risks industry executives should consider.

Finance: Although companies tend to dedicate the bulk of their anti-fraud resources to protection against financial crime, this remains the most exposed area. Currency exchange rates are essential to airline activity, especially for international firms. As such, relationships with brokerages require careful monitoring and companies should make sure that all activity fits strictly within the company's foreign exchange policy. Aircraft leasing contracts can also be a source of problems; managers should therefore regularly review contract terms and service performance. Background checks usually uncover red flags that are often not raised by day-to-day monitoring systems.

Marketing: The results of marketing are often the most intangible of any purchased service, so they are the hardest to evaluate and control. Service measurement techniques should include microeconomic analysis and market studies previously agreed in the contract with the service provider. Without these, although a contract may be technically fulfilled, companies might well pay more than the activities are worth.

Cargo: Cargo transportation has always been an important revenue source for airlines. Some, mainly small companies, however, do not have extensive cargo transportation departments and many airports lack proper storage facilities, making theft easier. Airway bills also require strict control. Incorrect weights or taxes on these bills can lead to losses. Moreover, false content declarations are both illegal and can put the whole company at risk.

REPORT CARD TRAVEL, LEISURE AND TRANSPORTATION

Financial Loss: Average loss per company over past three years \$10.2 million (116% of average)

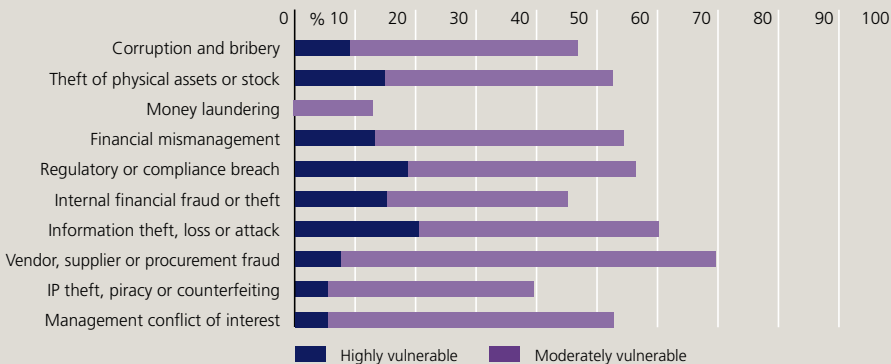
Prevalence: Companies suffering fraud loss over past three years 89%

Increase in Exposure: Companies where exposure to fraud has increased 83%

High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable to specific frauds
Information theft, loss or attack (21%) • Regulatory or compliance breach (19%)

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in past three years
Theft of physical assets or stock (47%) • Internal financial fraud or theft (32%) • Regulatory or compliance breach (30%) • Management conflict of interest (26%) • Information theft, loss or attack (23%) • Financial mismanagement (21%)

Investment Focus: Percentage of firms investing in this type of fraud prevention in the next year
IT security (60%) • Financial controls (57%) • Physical asset security (47%) • Management controls (38%)
Staff training (30%) • Due diligence (30%)





Ticketing: The rapid evolution of ticketing systems and related software has helped reduce fraud in this area. The ticketing process is still vulnerable to attack at numerous points, however, especially when payment is by credit card. Gangs specializing in card cloning use repeated ticket buying to obtain money. Corporate internal control systems should thus be synchronized with alerts issued by card companies. Moreover, credit approval systems must block suspicious transactions that are abnormal given the usual rate of regional card activity and the card holder's profile.

Maintenance: The acquisition of aircraft parts is crucial to an airline's success, often requiring precise logistical execution in the face of great urgency. Businesses in the sector live or die by their agility, and grounded aircraft mean lost income. For maintenance technicians, Aircraft on Ground (AOG) – means a top priority situation. Urgency, however, must not lead to those responsible for procurement compromising on the quality of parts or suppliers. Fake parts are distributed by suppliers which very often have no certification from civil aviation regulatory agencies. Checking a supplier's documentation, as well as researching market prices, can reveal irregularities.

Catering: Although on-board food services have seen reduced menus in recent years to allow airlines to lower ticket prices, effective controls in this area can still help companies avoid fraud and other losses. One useful approach is to occasionally reconcile, by route and type of aircraft, the number of on-board meals with the number of passengers. This practice often raises red flags of potential fraud.

Handling: The implementation of contracts for the use of equipment such as boarding ladders, push backs, power plants, and loaders for baggage handling must be thoroughly checked. Recording the time and equipment actually used provides useful data for certifying the fulfillment of contracted services. In a recent project, for example, it was noticed that during the loading of an A319 aircraft a luggage conveyor belt was not used, but the airline's auxiliary service provider charged for its use nonetheless.

Luggage: The logistics involved in luggage handling must be as efficient as all the other processes relating to the arrival and departure of aircraft. Mistakes can happen, and bags get diverted from the right destination. In some cases, however, we have found frauds varying from false content declarations to the issuing of refunds for supposedly lost luggage that was never checked. Moreover, despite automatic controls, repeated fraud related to excess baggage weight can cause considerable long-term losses.

Frequent Flyer Programs: Although not the most common cause of fraud in the sector, the abuse of mileage programs has seen considerable growth. In a recent investigation, we documented the improper transfer of miles to friends and relatives, data manipulation to improperly credit miles to unqualified individuals, and the sending of malicious emails to obtain data illegally and misappropriate the points of program members.

Information Technology: IT supports numerous aviation company procedures, from aircraft navigation, through ticketing, to financial management. Information systems are therefore targets for fraud. An investigation for an airline headquartered in Latin America identified a US\$10 million fraud that used a fake register of suppliers in the Enterprise Resource Planning system. Well designed policies, controls, password protocols, and accessibility rules, mainly for management software, can minimize risks.

This brief review underscores that airline companies need appropriate controls specific to each area of operation. They also need to align such controls with the creation of a compliance culture. Only through the commitment and support of every employee is it possible to reduce the levels of fraud within the aviation industry.



Vander Giordano is a managing director based in São Paulo and specializes in business development for Latin America. He is a member of the Brazilian and International Bar Associations and has worked in a number of areas in the airline industry.

EIU SURVEY

A worrying increase: Surveys from previous years indicated that fraud within the travel, leisure and transportation industry was a smaller problem than for many other sectors. This year the data are more of a cause for concern.

- While the average loss over the preceding three years has been growing slightly across the survey, in this sector it rose to \$10.2 million, or 116% of the average, dramatically up on the 2008 figures of \$2.5 million and 32%.
- The proportion of companies hit by any type of fraud declined only slightly, to 89% from 91%. This too exceeded last year's survey average (85%).
- Travel, tourism and leisure sector firms suffer from a broad range of incidences of fraud, rather than a dominant one. In the last three years, 47% experienced theft of physical assets – the third-highest rate of any industry; 32% faced internal financial fraud and 30% regulatory or compliance breaches, in both cases the greatest proportion of any sector; and 26% suffered from management conflict of interest, the second worst performance.

Contradictory spending: The industry is addressing the issue through greater anti-fraud spending, but efforts are inconsistent and hampered by cost-saving measures.

- This sector is traditionally near or above average in its deployment of anti-fraud measures covered in the survey. This should improve over the next 12 months. More sector firms than average expect to spend on seven out of ten of these measures, and in two of the other cases the difference is less than 1%. In particular, more companies plan to invest in enhanced asset security (47%) than in any other sector.
- Cost-cutting elsewhere, however, is leading to problems: 25% admit that efforts to save money have weakened internal controls and increased vulnerability to fraud, the worst result for any industry.
- The same number of companies say that pay restraint in the current environment has also raised such exposure, again a problem that is more widespread in this sector than anywhere else. This may, in turn, exacerbate the industry's traditional problem of high staff turnover, which 36% say has made them more susceptible to fraud this year.

Fraud is a growing problem for travel, transport and leisure companies, so they need to look not only at anti-fraud measures – which are already being undertaken by many companies – but also at consistent behaviour that minimizes fraud risks.

Written by The Economist Intelligence Unit



Three predictions for the future: The impact of the global economy on construction

Blake Coppotelli

In 1998, as part of the investigation into the metropolitan area's interior construction industry by the New York County District Attorney's Office, I cooperated one of the largest general contractors (CI) in the United States. The CI was a participant in the biggest kickback and bid-rigging cartel in the history of the New York City construction industry. He, along with approximately forty other individuals and companies, subsequently pled guilty to various felony crimes, including commercial bribery, after the inquiry uncovered pervasive bid-rigging on billions of dollars worth of private and public contracts.

During one of the initial debriefings of the CI, he explained the circumstances under which his participation in the cartel began. The dialogue went something like this:

Coppotelli: What brought about the bid-rigging?

CI: In 1989, the United States real estate market crashed. From 1989 through 1991 the opportunities dried up, but the competition remained the same. The larger firms were competing for practically no work, and struggling to win enough work to stay afloat, make payroll, and maintain our standard of living. We had to do something, so some of us decided to make sure that we won what work was out there.

Coppotelli: How did you do that?

CI: We contacted people who worked with and for our clients, and who were responsible for procuring contracts – project consultants and managers, designers, architects, engineers, and facility managers within our potential customer base. We talked to anyone who could steer the award of a contract and we offered to give them a cut of the action. We also hedged our bets and beat up on subcontractors to kick us back about 10 percent of their contracts enabling us, among other things, to reduce our pricing. It was easy. Everyone was in the same boat because of the collapse. Almost no one refused.

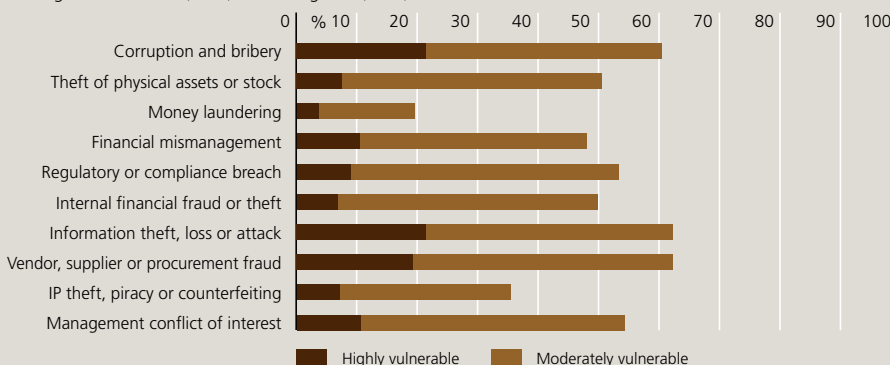
Over the course of the investigation, we negotiated the cooperation of over a dozen high level industry executives. Each told the same story. Most provided the following additional guidance, "You should also be focusing on the unions and organized crime. They have been affected just as much by the collapse of the market, and they have been hammering us. They are the ones controlling the labor costs. If organized crime controlled companies can cut their labor costs, it won't matter what we are doing, and they can do it easily by controlling, threatening or greasing the unions."

The investigation confirmed one critical fact: once the structure of fraud was in place, the criminal activity continued well past 1991 in spite of a market recovery. The schemes did not stop until they were uncovered by the investigation.

Since October, 2008, public and private construction around the world has suffered in unparalleled ways due to the global financial crisis. By January, 2009, the

REPORT CARD CONSTRUCTION

Financial Loss: Average loss per company over past three years \$6.4 million (73% of average)
Prevalence: Companies suffering fraud loss over past three years 91%
Increase in Exposure: Companies where exposure to fraud has increased 86%
High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable to specific frauds
 Information theft, loss or attack (21%) • Corruption and bribery (21%) • Vendor, supplier, or procurement fraud (20%)
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in last three years
 Corruption and bribery (38%) • Theft of physical assets or stock (36%) • Financial mismanagement (29%)
 Vendor, supplier or procurement fraud (25%) • Information theft, loss or attack (23%) • Regulatory or compliance breach (23%) • Management conflict of interest (21%)
Investment Focus: Percentage of firms investing in this type of fraud prevention in the next year:
 Financial controls (59%) • IT security (54%) • Physical asset security (39%) • Staff training (39%)
 Management controls (36%) • Due diligence (34%)



American Institute of Architects Consensus Nonresidential Construction Forecast Panel predicted that office, hotel, and retail projects would decrease over the next two years by 28.8, 25.8, and 32.4 percent respectively. Global Insight said that the same sectors over the next two years would decline by 38.1, 40.0, and 34.1 percent. Moody's Economy.Com put the expected drops at 45.6, 21.5, and 35.7 percent, and FMI at 36.3, 31.8, and 56.7 percent. All four have increased their pessimism in one sector or another as the year has progressed. These numbers reflect the condition and future of the United States construction industry. Clearly, its current state has eclipsed that of the 1989 to 1991 collapse, and looks set to worsen in the years to come.

So, what can history teach us? Here are three predictions for the next three years:

Fraud will increase dramatically in the private commercial construction industry. Collusive bidding, bid-rigging, kick-backs, and billing schemes for core and shell and interiors work will increase significantly by necessity. There will be a resurgence of "pay to play" practices or companies will be forced out of business.

Fraud will increase substantially on public contracts, particularly infrastructure projects. The federal stimulus package will act like a magnet, drawing ethical and corrupt alike, and will favor the dishonest as political and public corruption, collusive bidding, bid-rigging, and prevailing wage violations flourish.

Labor Racketeering and organized crime activities will rise sharply on both public and private contracts. Unscrupulous union representatives and/or organized crime controlled unions will increase their activities, allowing corrupt and/or organized crime controlled companies to violate their collective bargaining agreements, particularly their union wage rates, or prevailing wage requirements, so that they can lower their labor costs and underbid honest competitors.

Make no mistake. Consistent with historical precedent, corrupt contractors, labor officials, and organized crime have spent the past nine months planning, organizing, and coordinating their activities to survive the current economic downturn. These players look to government stimulus contracts as a vital source of revenue, a once in a decade opportunity that they will seize at any cost. They have been actively planning and coordinating their efforts, and cultivating political connections. Their tactics and planning place them well ahead of their competition's legitimate business initiatives. What is more, federal and state

law enforcement efforts currently in place to combat this behavior as well as the accountability initiatives of the federal and state agencies overseeing the distribution and use of the stimulus funds are outdated and arguably inadequate.

So, what recourse is there? Federal and state agencies need to do more than just institute the safeguards promulgated by the Recovery Accountability and Transparency Board. Those requirements, and the Board's checklist, will not prevent collusive bidding, kickbacks, public corruption, and labor or material misuse abuses. These agencies and the private sector need to supplement their current resources and enlist or employ construction fraud experts to:

- monitor procurement proactively;
- forensically analyze the scope of work and costs submitted in bids;
- conduct detailed anti-fraud related background investigations on vendors and their principles or key managerial agents;
- forensically examine the legitimacy of costs in all requisitions or invoices as well as of those underlying change orders and "time and material" work;
- institute investigative oversight of work performed, including the integrity of labor and materials used on the project;
- require complete transparency in the disclosure and tracking of all vendor costs;
- enhance intra- and inter-agency communication to facilitate the sharing of critical information related to vendors and, to the extent possible, information related to active or planned criminal investigations.

Agencies and the private sector should not rely on project auditors, project consultants, or construction managers to conduct this work. Although they say that they provide integrity monitoring services, project auditors reconcile contracts against work completed and costs incurred, and do not conduct fraud analysis. Construction managers and project consultants have numerous conflicts of interest in handling these anti-fraud tasks, do not have any fraud detection or prevention expertise, and potentially should be part of the group monitored.

The message, then, is "praemonitus, praemunitus," forewarned is forearmed.



Blake Coppotelli is a senior managing director of Business Intelligence & Investigations and head of Real Estate Integrity services based in New York. A former prosecutor for 13 years, he served as chief of the Labor Racketeering Unit and Construction Industry Strike Force in the Manhattan District Attorney's office.

EIU SURVEY

Fraud levels are down: This sector traditionally has a widespread fraud problem. Since the last survey, the level of financial loss to fraud has abated significantly, owing most likely to the substantial decline in construction contracts in 2009.

- The average loss per company to fraud over the last three years was \$6.4 million, or 73% of the survey average. This represents a significant decline on the 2008 survey figure of \$14.2 million
- The prevalence of the problem, however, is not declining at nearly the same speed: 91% of construction, engineering and infrastructure companies were hit by some form of fraud in the last three years, down slightly from the 2008 proportion of 95%, but still well above the survey average of 85%.
- The types of fraud incidences are also changing, sometimes dramatically. For example, 38% experienced corruption and bribery, up from 28% in the last survey. This was the highest figure of any sector, no doubt because so much of current available work is government funded.
- Other frauds declined in prevalence, such as management conflict of interest from 29% to 21%.

Awareness of the problem: Although sector companies realize that they have a problem, these shifts help to explain why their efforts are not always focused in the right areas.

- The sector has the highest proportion of firms calling themselves highly vulnerable to vendor fraud (20%) and the second highest to corruption and bribery (21%),
- Sector companies are more likely than average to invest in eight of the ten anti-fraud strategies in the survey, and are leading all others in spending on financial controls (59%) and staff training (39%).
- Conversely, although regulatory breaches are relatively widespread in this industry, only 9% of firms believe that they are highly vulnerable to the problem – below the survey average of 13%.

Contradictory effects of the downturn: The impact of the downturn and the demands of survival are throwing up particular challenges beyond greater levels of corruption.

- 34% believe that the financial crisis has increased the level of fraud at their organizations and 16% say reduced revenues or growth are in themselves making them more vulnerable to fraud.
- Some of the demands of the industry, exacerbated by current conditions, are causing particular difficulties: the sector has the highest percentage of companies where high staff turnover is increasing vulnerability to fraud (38%), as well as the highest figure for those saying greater collaboration is contributing to the problem (27%).

As the downturn reshapes the fraud picture and increases vulnerability, it may also be responsible for the reduction in financial losses. Whereas over one-third said that the economic situation was creating more fraud, only 20% had seen an overall increase in levels of fraud at their companies, compared with 31% who had seen a decrease in the last year. Here, as elsewhere, there simply may be less money to steal. Overall, the sector's vulnerabilities are growing even while its losses are declining.

Written by The Economist Intelligence Unit

Fraud heatmap: where the pain is, and how it reacts

As in previous surveys, we have attempted to plot significant areas of fraud loss for particular sectors using a heatmap. The pattern that emerges is clear and straightforward – each sector has its own risk profile, typically caused by its exposure to risk from clients, suppliers, staff and governments or regulators. These dictate the types of threat it faces from fraud. The grid in Figure 1 averages the findings from Kroll’s Global Fraud Surveys in 2007, 2008 and 2009 and it shows specific fraud threat by sector. We have regarded a sector as especially highly exposed if its exposure is higher than other sectors. So calling money

laundering a high threat to financial services reflects the fact that it experiences this more than other sectors, not that money laundering is common in banking (it isn’t).

What also emerges is that some fraud threats are relatively pervasive – most sectors experience them at different times: theft of assets or stock, financial mismanagement, and (a sign of changing times) information theft, loss or attack and IP theft, privacy or counterfeiting. These are the most basic forms of fraud. Others are more specific to certain sectors: corruption and bribery, regulatory and compliance breach apply to sectors with government as

“Corruption and bribery and regulatory and compliance breaches apply to sectors with government as a regulator or client”

a regulator or client. Internal financial fraud or theft affect businesses in particular where cash and cash handling is important (financial services, retail, wholesale and distribution, and travel, leisure and

Figure 1: Fraud experienced by survey respondents by sector

	Financial services	Professional services	Manufacturing	Healthcare, pharmaceuticals & biotechnology	Technology, media & telecoms	Natural resources	Travel, leisure & transportation	Retail, wholesale & distribution	Consumer goods	Construction
Corruption and bribery	16%	14%	24%	13%	16%	24%	20%	22%	19%	33%
Theft of physical assets or stock	28%	23%	46%	35%	30%	43%	43%	51%	44%	37%
Money laundering	11%	4%	4%	4%	3%	4%	6%	2%	1%	5%
Financial mismanagement	25%	17%	24%	24%	17%	17%	22%	21%	15%	30%
Regulatory or compliance breach	28%	17%	21%	30%	17%	21%	21%	14%	21%	25%
Internal financial fraud or theft	27%	10%	19%	18%	9%	20%	28%	22%	18%	17%
Information theft, loss or attack	25%	28%	23%	22%	29%	24%	23%	25%	22%	19%
Vendor, supplier or procurement fraud	12%	16%	21%	18%	17%	21%	19%	25%	28%	23%
IP theft, piracy, or counterfeiting	7%	15%	21%	20%	19%	11%	9%	14%	21%	9%
Management conflict of interest	23%	23%	18%	24%	15%	33%	30%	18%	18%	24%

We have calculated the “hot spots” relative to how common a fraud threat is. So: a small proportion of financial services companies are confronted by money laundering, but this is very high compared to every other sector, so it is a “hot spot”. And: a relatively high proportion of financial services companies face theft of physical assets or stock, but this is much lower than, say, manufacturing or retail, so it is not a “hot spot”.

The industry feels the

transportation). Vendor fraud strikes those businesses with extended or complex supply chains (construction and engineering, consumer goods, and retail, wholesale and distribution). Money laundering is quite specific to financial services, with lower levels of incidence in a couple of other areas. It figures, therefore, that each industry has its own profile when it comes to fraud countermeasures. Banks need more elaborate measures to safeguard their finances than consumer goods companies, but they don't need to spend as much on IP protection. Figure 2 shows the pattern of measures they have taken. Some areas

(financial controls, physical security, IT security and protection of assets) are generic protection against several kinds of threat. Others (due diligence, staff screening, IP protection) are specific to sectors that face complex supply chains, sensitive internal issues or regulation or high-value IP. Together, this mixture of threat and counter-measure makes for the risk profile of the industry concerned. Each has prioritized the threats it faces and the measures it is ready to take to prevent, detect or mitigate them.

“Banks need more elaborate measures to safeguard their finances than consumer goods companies, but they don't need to spend as much on IP protection”

Figure 2: Fraud countermeasures adopted by survey respondents by sector

	Financial services	Professional services	Manufacturing	Healthcare, pharmaceuticals & biotechnology	Technology, media & telecoms	Natural resources	Travel, leisure & transportation	Retail, wholesale & distribution	Consumer goods	Construction
Financial: financial controls, fraud detection, internal audit, external audit, anti-money laundering policies	92%	69%	89%	85%	69%	89%	85%	73%	93%	86%
Staff: background screening	60%	41%	41%	53%	48%	43%	53%	42%	26%	36%
Staff: training, whistleblower hotline	48%	25%	50%	51%	34%	59%	43%	38%	50%	45%
Partners, clients and vendors: due diligence	49%	48%	53%	50%	38%	57%	40%	37%	41%	46%
Reputation: media monitoring, compliance controls and training, legal review	55%	31%	46%	44%	48%	50%	43%	31%	46%	38%
Risk: risk officer and risk management system	67%	25%	36%	44%	35%	54%	45%	27%	35%	38%
IP: intellectual property and trademarks monitoring programme	26%	21%	47%	47%	41%	39%	25%	21%	57%	32%
Assets: physical security systems, stock inventories, tagging, asset register	63%	66%	81%	65%	58%	80%	70%	69%	83%	73%
Information: IT security, technical countermeasures	76%	58%	74%	74%	83%	80%	77%	67%	70%	68%
Management: management controls, incentives, external supervision eg, audit committee	70%	48%	80%	62%	56%	73%	58%	54%	59%	73%



Corruption fears grow

Corruption and bribery are rising rapidly up the list of fraud issues worrying companies, the Kroll Global Fraud Survey shows. This year, concern about it has increased from around 11 percent of respondents to nearly 14 percent. The greatest concern remains information theft, loss or attack. Just over 20 percent of respondents consider themselves highly vulnerable to this issue, but that is down from nearly 25 percent last year. IP theft, piracy and counterfeiting have also declined as concerns.

Theft of physical assets or stock – which, the survey shows, is the most common form of loss – is also rising up the list of corporate concerns.

Percentage of companies which consider themselves highly vulnerable to specific frauds

	2009	2008
Corruption and bribery	13.9%	10.9%
Theft of physical assets or stock	13.5%	11.5%
Money laundering	4.8%	4.7%
Financial mismanagement	10.7%	9.6%
Regulatory or compliance breach	12.8%	12.3%
Internal financial fraud or theft	8.8%	7.7%
Information theft, loss or attack	20.1%	24.5%
Vendor, supplier or procurement fraud	11.5%	10.3%
IP theft, piracy or counterfeiting	12.8%	16.9%
Management conflict of interest	10.7%	13.2%

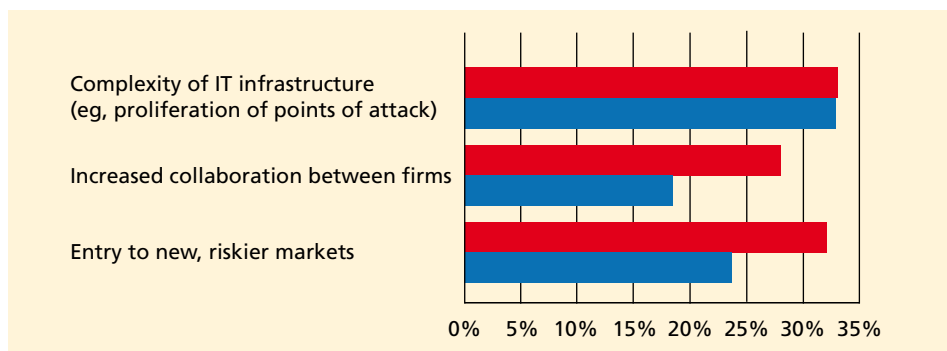
Slowdown in business expansion drives reduction in fraud factors

Why should fraud fall during a downturn? The answer is that as economic activity – particularly the more risk-seeking, enterprising sort – falls, so do the opportunities and drivers for fraud.

We asked respondents to our survey which activities they believed had increased their exposure to fraud.

The chart below illustrates the answers. The answers vary by sector, but clearly complexity of IT infrastructure is a significant factor especially for financial services. Entry to new and riskier markets is important for several sectors – manufacturing, natural resources, and to a lesser extent construction and engineering, and financial services. High staff turnover hits a number of sectors.

Three drivers of fraud



North America**Consulting Services**

David Holley
Boston
1 617 350 7878
dholley@kroll.com

Jeff Cramer
Chicago
1 312 681 1500
jrcramer@kroll.com

Ken Mate
Los Angeles
1 213 443 6090
kmate@kroll.com

Robert Brenner
New York
1 212 593 1000
rbrenner@kroll.com

Blake Coppotelli
New York
1 212 593 1000
bcoppotelli@kroll.com

Bill Nugent
Philadelphia
1 215 568 2440
bnugent@kroll.com

Betsy Blumenthal
San Francisco
1 415 743 4800
bblument@kroll.com

David Hess
Reston, VA
1 703 796 2880
dhess@kroll.com

Kroll Ontrack

Tony Cueva
Eden Prairie
1 952 949 4156
tcueva@krollontrack.com

Identity Theft

Brian Lapidus
Nashville
1 615 320 9800
blapidus@kroll.com

Background Screening

Scott Viebranz
Nashville
1 615 320 9800
sviebranz@kroll.com

Latin America**Consulting Services**

Sam Anson
Miami
305 789 7100
sanson@kroll.com

Andres Otero
Miami
+1 305 789 7100
aotero@kroll.com

Vander Giordano
São Paulo
+55 11 3897 0900
vgjordano@kroll.com

Eduardo Gomide
São Paulo
+55 11 3897 0900
egomide@kroll.com

Matias Nahon
Buenos Aires
+54 11 4706 6000
mnahon@kroll.com

Glen Harloff
Grenada
+473 439 7999
gharloff@kroll.com

David Robillard
Mexico City
+52 55 5279 7250
drobillard@kroll.com

Asia**Consulting Services**

Tadashi Kageyama
Hong Kong
852 2884 7725
tkageyama@kroll.com

Tsuyoki Sato
Tokyo
81 3 3218 4875
tsato@kroll.com

Nick Blank
Seoul
82 2 2021 2700
nblank@kroll.com

Violet Ho
Beijing
86 10 5964 7666
vho@kroll.com

Richard Dailly
Mumbai
91 22 4244 0501
rdailly@kroll.com

Chris Leahy
Singapore
65 6327 7642
cleahy@kroll.com

Background Screening

David Liu
Hong Kong
852 2884 7716
dliu@kroll.com

Kroll Ontrack

Data Recovery
Adrian Briscoe
Brisbane
61 732 551 199
abriscoe@krollontrack.com

Legal Technology

Ben Pasco
Hong Kong
852 2884 7769
bpasco@kroll.com

Europe, Middle East & Africa (EMEA)**Consulting Services**

Richard Abbey
London
44 207 029 5000
rabbey@kroll.com

Brendan Hawthorne
London
44 207 029 5482
bhawthorne@kroll.com

Max Cawdron
Madrid
34 91 274 79 53
mcawdron@kroll.com

Bechir Mana
Paris
33 1 42 67 81 46
bmana@kroll.com

Tom Everett-Heath
Dubai
971 43050620
teverettheath@kroll.com

Marianna Vintiadis
Italy
39 02 8699 8088
mvintiadis@kroll.com

Background Screening

Tony Shepherd
London
44 7917 857913
tshepherd@kroll.com

Kroll Ontrack

Tim Phillips
London
44 207 549 9600
tphillips@krollontrack.co.uk

Headquartered in New York with offices in more than 60 cities in over 29 countries, Kroll has a multidisciplinary team of more than 3,000 employees and serves a global clientele of law firms, financial institutions, corporations, non-profit institutions, government agencies, and individuals. Kroll is a subsidiary of Marsh & McLennan Companies, Inc. (NYSE: MMC), the global professional services firm.

Experts in fraud intelligence and investigations

For over 35 years, we have helped our clients to prevent, investigate and recover from fraud. We specialize in investigation, forensic accounting and computer forensics. Whether your problem is global, local or cross-border, we design solutions from our range of services, which include:

- Corporate Internal Investigations
- FCPA, Regulatory & Corporate Governance Investigations
- Forensic Accounting
- Compliance Monitoring
- Asset Tracing & Recovery
- Intellectual Property Protection
- Litigation Support
- Fraud Prevention Training
- Process & Internal Controls Assessment
- Computer Forensics
- Expert Testimony
- Investigative Due Diligence
- Electronic Discovery
- Government Contractor Advisory Services
- Identity Theft Restoration
- Real Estate Integrity Services
- Anti-Money Laundering Programs
- Loss Prevention

Kroll also provides services in

- Security Consulting
- Background Screening
- Data Recovery & Legal Technologies
- Business Intelligence
- Hostile Takeover, M&A and Hedge Fund Intelligence
- Employee & Vendor Screening