

Global Fraud Report



Global and local issues discussed.

Sector by sector analysis.

Economist Intelligence Unit overview.

Prevention, detection & response.

Kroll commissioned The Economist Intelligence Unit to conduct a worldwide survey on fraud and its effect on business during 2007.

A total of 892 senior executives took part in this survey. A third of the respondents were based in Europe, 32% in Asia-Pacific and 30% in North and South America. 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 (18%) followed by professional services (11%) and manufacturing (11%). Fully 38% 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.

Please note that some of the names and events have been changed in Kroll case studies to prevent identification of subjects and clients.

While every effort has been taken to verify the accuracy of this information, neither The Economist Intelligence Unit Ltd., Kroll nor their affiliates can accept any responsibility or liability for reliance by any person on this information.

© 2007 The Economist Intelligence Unit and Kroll. All rights reserved.

Global Fraud Report

INTRODUCTION	2	CONSUMER	22
CHAIRMAN'S VIEW	3	Brand integrity:	
The sharp rocks under the water	3	Anti-counterfeiting, piracy and tainted goods	22
EIU OVERVIEW	4	CONSTRUCTION	24
The Economist Intelligence Unit overview	4	Audits, screening, and expertise help to build integrity	24
FINANCIAL SERVICES	6	Transparency is the key to monitoring the supply chain	25
Identity theft prevention: A looming requirement	6	Red Flags:	
Operation Malaya:		Behavior that may reveal problems	26
Corruption in the Spanish real estate sector	7	FRAUD VULNERABILITY	27
Private equity, hedge funds and emerging markets:		Where business is feeling the heat	27
Playing risk for returns	8	EMERGING MARKETS	28
Alternative securities:		The investment herd stampedes into Lagos:	
Opportunity for fraud and reward	9	Dangers of fraud in a booming market	28
PROFESSIONAL SERVICES	10	The impact of United States regulation on other countries	29
Preventing risk in the people business	10	Culture, compliance and China	30
MANUFACTURING	11	FRAUD PREVENTION	31
Procurement data can help fight fraud	11	A proactive strategy for operational risk	31
HEALTHCARE, PHARMACEUTICALS & BIOTECHNOLOGY	12	Human resources:	
Hijacking pharmaceutical brands:		The frontline in protecting your business	32
A study	12	Protecting your investments	33
Counterfeiting in the pharmaceutical industry:		FRAUD DETECTION	34
Ten pieces of advice	13	Up to the top: Financial statement fraud	34
TECHNOLOGY, MEDIA & TELECOMS	14	Protecting data sources from internal theft	35
Machinations in the Japanese entertainment industry	14	Making employee hotlines work	36
Old-fashioned fraud:		FRAUD RESPONSE	37
A case study from China	15	Investigative tactics under scrutiny in the United States	37
NATURAL RESOURCES	16	Who is taking responsibility for losing sensitive data?	37
Challenging corruption in the energy sector	16	U.S. Government increases controls over contractors	38
TRAVEL, LEISURE & TRANSPORTATION	18	Profiting from stolen information	39
Unique profile of the airline industry	18	KROLL CONTACTS	40
The gambling industry and money laundering	19	KROLL SERVICES	41
RETAIL, WHOLESALE & DISTRIBUTION	20		
Commodity trading and shipping fraud	20		
Working out weak points can pay off	21		

Introduction



Andrés Antonius is President of Kroll's Consulting Group and previously occupied high ranking positions in the Mexican Government. He holds a Ph.D in Economics from Harvard University

The risk of fraud is a part of doing business. It can even be considered a consequence. No further evidence is needed than a glance at the business section of any major newspaper any day of the week. The appearance of fraud at a company is not necessarily, or even usually, a sign of negligence or ethical laxity at the top. It is instead often the result of large, complex organizations doing business in many different venues, currencies, legal frameworks, and cultures, often at the same time. This context creates severe challenges for today's managers, legal counsels, and compliance officers, who must be all-seeing and all-knowing, and never sleep.

While frauds have existed throughout history, one might argue that the risks of fraud for business are greater today than in the past. Recent events, be they the bankruptcies of once fabled companies such as Enron or Worldcom, the manipulation of the financial system by drug traffickers and terrorists, or the emergence of complex derivatives, have heightened the sensitivities of authorities, regulators, and the investing public. Even the whiff of a fraud may sometimes be sufficient to place a company under severe scrutiny or in financial distress.

However challenging this context may be, strategies exist to minimize the risks in any given industry or situation. All of them have a common starting point: the explicit and declared intent by management to make fraud detection and prevention a top corporate priority. Any strategy which fails to emphasize this point will necessarily be limited in its success.

Edmund Burke famously said "The only thing necessary for the triumph of evil is for good men to do nothing." In the fight against fraud, complacency is often the biggest obstacle. Complacency regarding fraud arises for many reasons, but mostly because some see the inevitability of fraud occurring as evidence that it cannot be prevented. This confusion may itself create an atmosphere of tacit acceptance, or at least one in which the questioning of certain decisions or transactions is frowned upon and seen as an impediment to doing business, when in fact it is often the opposite.

Complacency is also sometimes paradoxically the result of operating in

mature economies and markets. While the belief often exists that fraud and corruption are greatest in foreign cultures or emerging markets, the largest frauds in history have taken place in the developed world, in economies with highly evolved legal and regulatory systems which exact severe penalties against fraudsters. Both companies and investors logically tend to be more cautious and vigilant when examining business operations or opportunities in countries which are unfamiliar to them. But sometimes they forget that just like car accidents, most fraud occurs close to home.

It may be that fraud is perceived as more prevalent in emerging markets. But without doubt the severity of it – the cost, and the reputational impact – is as high, or higher, in developed economies.

This first annual *Global Fraud Report* presents the collective knowledge of some of the world's most talented and diligent fraud fighters. Kroll's team of experts is composed of top forensic accountants, computer forensic and IT specialists, former leading prosecutors, regulators, law enforcement and intelligence officers, and some of the most distinguished investigative journalists in the market. They represent decades, if not centuries, of experience in fraud prevention and detection. And the diversity of their skill sets and international backgrounds means that they can effectively address any situation in any locale in the world.

The *Global Fraud Report* also contains a fascinating survey carried out by The Economist Intelligence Unit which provides insights into the frauds that have the most impact on companies around the world and the top risks that today's managers perceive. One survey result that stands out is that while internal financial fraud was reported as one of the most pervasive and frequent types of fraud, it was not considered as important a threat as information theft, money laundering, or the theft of physical assets. Is this not itself evidence of the complacency we must avoid?

A stylized, handwritten signature in dark ink, appearing to read 'A. Antonius'.

ANDRÉS ANTONIUS

The sharp rocks under the water



Recent months have shown that turbulence in financial markets reveals rocks at the bottom of the stream. They have always been there, but only when the water level drops do the sharp edges become exposed.

Financial instruments that are overly complex and not understood by many, unregulated players and the creditworthiness of counterparties in certain sectors have already been exposed as major vulnerabilities. Numerous frauds will be uncovered at a time like this and then the finger pointing will begin. As usual, the presence of fraud emerged once the water level dropped precipitously.

Throughout the 35-year history of Kroll Inc., our mission has been to help our clients achieve greater transparency and a deeper understanding of the underlying facts in a range of situations and to assist with solutions.

When one reviews some of the results from this latest survey on fraud, it is clear that certain types of exposures have increased and that all of the old ones persist to some degree. As our society has become more reliant on information technology, increased globalization and greater interconnectedness, certain exposures have expanded right along with them. Dramatically new frauds, such as ID theft,

various IT crimes and false reporting by asset managers, were rarely seen 25 years ago. The expansion of economies and dramatic increases in liquidity have also opened the door to problems becoming more substantial, based on scale and the speed of activity. Fraud occurs to a far greater extent away from the home office and more distant operations create a disproportionate number of incidents. Controls are more difficult to regulate and there are fewer people “minding the store” in these remote locations. The examples in the 1990s included Daiwa, Sumitomo, Barings, and Bre-X. These all occurred at a distance from the home office, although fraud can also be perpetrated at the center.

Much of today's effort to control exposure to fraud is driven by administrative regulations, accompanied by criminal enforcement. As the stakes have gone up, many societies have increasingly criminalized activities that 25 or 30 years ago would have been dealt with administratively, such as accounting restatements and insider trading. The policing of these matters has often arisen from new laws, such as Sarbanes-Oxley and related rules, which came about as a direct result of some of the more notorious frauds that were uncovered from 2000 to 2003 such as those at Enron, WorldCom, Ahold, Parmalat and others. As one can see from the results of our commissioned survey and recent headlines, institutional exposure to fraud does not seem to be lessening despite substantial increases in oversight activity both internally and by third parties, such as the audit profession and specialized organizations such as Kroll.

As we look ahead, it is clear that the increased use of information technology tools combined with dramatic growth in the world economy will lead to more challenging times. Nowhere will the effect be greater than in the newly developing markets where growth continues to be very significant. The culture of these societies, best epitomized by the BRIC countries (Brazil, Russia, India, China) will be challenging, if profitable, for a new generation of entrepreneurs. We should pay particular attention to the integrity of the financial information since many companies in these economies have

traditionally had opaque financial systems. The sheer growth of these economies provides a greater opportunity for corruption, false accounting, and other aberrational activities. The controls are under greater stress, the pace of activity is more intense, and the reward system often based on output and profitability rather than controls and ethical behavior.

The multinational corporations and institutions that plan for further expansion in emerging markets need to devote a greater share of their control efforts to certain major risks:

- Corruption is endemic in some countries and it will take many years for that to change. The recent rise in the number of Foreign Corrupt Practice Act (FCPA) cases in the U.S. is a testament both to increased activity by law enforcement as well as to intense competition for markets. Further complicating these cases is the wide variation in the extent of the rule of law in BRIC countries. China has historically had weaknesses in its judicial system but it is progressing, as is Russia. Brazil and India are much further along the road toward established legal systems, but allegations of judicial corruption remain common.
- Second, there is a broad-based effort in certain countries to misappropriate the intellectual property of the companies that developed it. The lack of a proper legal system is aiding this type of fraud and alternative deterrents will have to be developed. Counterfeiting is only one aspect of the problem, but it is becoming more perilous as pharmaceuticals and critical equipment are being copied. These counterfeits can kill and in recent months China has begun to address the issue slowly.
- Third, there is a continuing series of IT-based frauds that will multiply and cause more substantial damage. These exposures range from ID theft, misappropriation of assets and information, wholesale financial embezzlement and the manipulation of accounts or even trading systems.

Technology, as my friend Sir Martin Sorrell recently said, is our “Frenemy.” It can be the tool which is used to commit the act or to unearth the crime. I hope we will use our resources to train and our technology to arm against the constant threat of fraud in the future.

JULES B. KROLL



Economist Intelligence Unit overview

Although often reluctant to discuss it, almost every business will at some point have been the victim of corporate fraud. The extent to which industries experience different categories of corporate fraud varies according to the nature of their business. For example, companies that deal with physical assets, such as consumer goods and retail, are more likely to suffer from the theft of physical assets or supplier fraud. Meanwhile, those that operate in the “knowledge economy”, such as professional services or technology, are more likely to be concerned about information theft or intellectual property issues.

Industries also vary in terms of the extent to which they are addressing the problem. For example, financial services which, given the nature of their business, face especially acute threats from internal financial fraud or money laundering, are obliged from a regulatory perspective to demonstrate that they have strong controls in place. Less heavily regulated industries may not have this impetus, but they nevertheless are likely to adopt some measures – whether financial controls or information technology (IT) security – to prevent or detect fraudulent activity.

The objective of this report is to examine the problem of corporate fraud, both for

business in general and within particular industries, and to explore the approaches that companies take to minimize their exposure to these threats. The findings are based on a survey, commissioned by Kroll, of nearly 900 senior executives worldwide, 40% of whom are C-level, or board-level executives. The key findings include the following:

Corporate fraud is a serious, widespread challenge that takes multiple forms:

- In the past three years, four out of five firms have suffered from some form of corporate fraud. Particularly widespread is the theft of physical assets or stock, which was experienced by 34% of surveyed respondents, while one-fifth of firms suffered from information theft, management conflict of interest, financial mismanagement, internal financial fraud, procurement fraud, and corruption and bribery.
- Over the same period, the average damage from corporate fraud among large companies – defined as those with an annual turnover of more than \$5 billion – was more than \$20 million, with about 1 in 10 losing more than \$100 million.
- The theft of, loss of, or attacks on information are a major concern, with 20% of respondents describing themselves as highly vulnerable here and 31% believing that IT complexity has increased their exposure to fraud.
- More generally, nearly half of companies rank themselves as at least moderately vulnerable to a very wide range of threats: regulatory or compliance breach (50%); management conflict of interest (49%); financial mismanagement (49%); procurement fraud (47%); theft of physical assets (47%); corruption and bribery (46%); and intellectual property (IP) theft (45%).

The prevalence of corporate fraud has held steady recently, but new business models driven by globalization are increasing exposure at most companies:

- Respondents are divided as to whether corporate fraud is on the increase. Roughly one-third of those surveyed think that the prevalence has stayed the same, one-third say that it has increased, and one-third say that it has decreased.
- Eighty-one percent of firms report that their exposure to corporate fraud has grown.

- The most frequent cause of this increased exposure is high staff turnover, which is cited by 32% of respondents. Close behind are complex IT arrangements (31%), entry into new markets (28%) and increased collaboration between firms (26%) – all of which are factors that are closely tied with modern business practice. Entry into new markets is of particular concern for larger firms (38%).

Companies treat corporate fraud as largely a financial and IT issue, but too many are insufficiently prepared for these and other risks:

- Most businesses (58%) give the internal audit/finance function the lead role in dealing with corporate fraud. The most widespread strategies used to combat the problem are financial controls (used in this respect at 79% of firms) and IT security (70%). This approach makes sense, as many of the biggest fraud problems relate to finance and technology.
- The same numbers suggest, however, that a surprising 21% of firms do not use financial controls for this purpose and 31% do not use IT security.
- These strategies also only indirectly address the most frequent form of corporate fraud – theft of physical property – against which only two-thirds of firms have measures in place to protect themselves.

Although this report focuses on differences in corporate fraud between sectors, certain risks are far more strongly correlated with company size and location:

- Larger companies are obviously bigger targets. On average, they lose six times more money to corporate fraud than smaller ones.
- The extent of corruption and bribery varies widely from one region to another. The proportion of firms that has recently suffered from it in the Middle East and Africa (39%) is by some distance the highest. But more than twice as many Eastern European respondents have experienced the problem than those from Western Europe, (14%), and more than three times as many from Latin America (29%) as from North America (9%).
- Internal financial fraud shows a similar geographic pattern: Middle East and Africa (46% of firms), Eastern Europe

(28%), Western Europe (18%), and North America (14%).

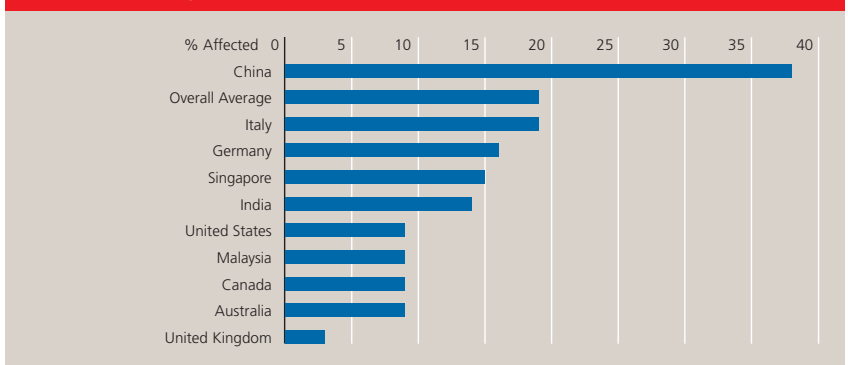
- Regional variations with intellectual property theft and counterfeiting are closely linked to countries rather than regions. Among firms operating in the China, 38% have experienced such fraud in the past three years, compared with just 14% in rival developing economy India. The latter compares favorably with the overall figure of 19%, and even the 9% reported among Canadian and U.S. respondents. That one in eleven firms in the latter still suffer from this problem, however, speaks of relative rather than absolute success in addressing it.

The frequency of the most widespread types of corporate fraud, and those giving rise to the most concern, vary relatively little by region:

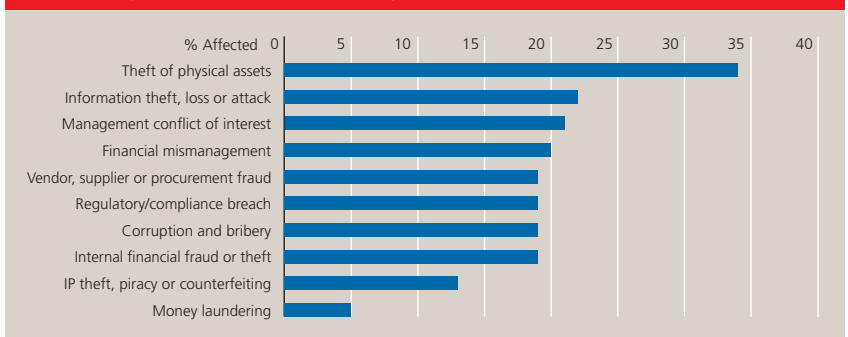
- Theft of physical assets was reported by between 32% and 40% of firms in all regions.
- Between 24% and 31% of companies had suffered information attack in most areas, except North America (16%) and Latin America (18%).

Economist Intelligence Unit

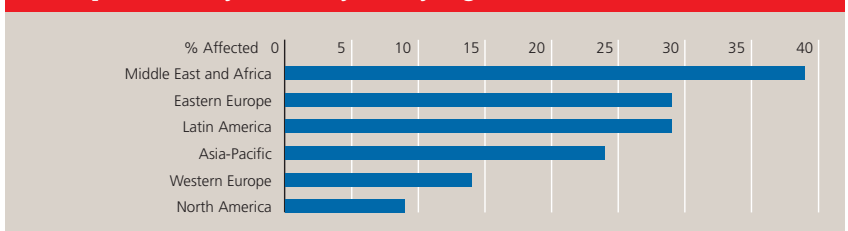
Percentage of companies affected by IP theft in last 3 years in selected countries



Percentage of companies suffering from various types of frauds in last 3 years



Percentage of companies suffering from corruption/bribery in last 3 years by region



Identity theft prevention: A looming requirement?



Identity theft is a rapidly growing problem for financial institutions and their customers. More than 600,000 consumers become victims each year in the U.S. alone, and four of the top five techniques involve financial services: opening new credit card accounts; using existing ones; opening new deposit accounts; and obtaining loans. Financial institutions will increasingly absorb much of the economic loss from this kind of fraud.

In the past, many banks have not involved themselves, other than to sympathize with affected customers. Even as the frequency of identity theft issues has risen, many banks have thought it sufficient to assist victimized customers by giving them telephone numbers to call, directing them to the appropriate credit bureau agencies, or providing other advice on what the customers could do for themselves.

In July 2006, however, the United States federal financial institution regulatory agencies and the Federal Trade Commission

released a proposed new federal rule, commonly known as the “Red Flags Rule”. The proposal, if adopted, would require financial institutions to put in place a written identity theft program emphasizing the detection, prevention, and mitigation of this crime. The program would have to contain reasonable policies and procedures to address the risk of identity theft in order to protect customers as well as the bank.

The proposal outlines, in some detail, 31 patterns, practices, and specific types of activity that should raise a “red flag”, signaling a risk of identity theft in connection with an existing account or the opening of a new one.

The proposal would require financial institutions to:

- Verify the identities of persons opening accounts;
- Identify red flags relevant to possible risks of identity theft which could harm customers or the safety and soundness of the institution or creditor;

- Detect these red flags in connection with the opening of an account or activity in any existing account;
- Assess whether these detected red flags prove a risk of identity theft;
- Mitigate this risk as appropriate for its degree;
- Train staff to implement the Red Flag Program;
- Oversee service provider arrangements;
- Specifically for credit and debit card issuers, develop policies and procedures to assess the validity of a request for a change of address followed closely by a request for additional or replacement cards.

How do financial institutions feel about this proposed rule? Not surprisingly, in the wake of the U.S. A Patriot Act, further compliance burdens have not been well received, especially when some already form part of Customer Identification Programs. In addition to the outlined obligations, there will undoubtedly be additional information security burdens as well.

Happy or not, although the rule has not been finalized, financial institutions are on notice of what some agencies contend should be minimum standards. Institutions should be taking steps now to prepare programs that will prevent the theft of customers’ identities. It is ultimately a small price to pay for maintaining their own safety and soundness while building loyal customer relationships and implementing strong prevention programs.

Liz Marchese is a director in Miami. She has over 20 years of banking operations, security and compliance experience, most recently at Union Planters Bank. She has served three times as president of the Financial Institutions Security Association (FISA) and is a qualified expert witness.

REPORT CARD FINANCIAL SERVICES

Financial Loss: Average loss per company over past three years: U.S.\$14.6m (218% of average)

Prevalence: Percentage of companies suffering corporate fraud loss over past three years: 83%

Increase in Exposure: Percentage of companies where exposure to fraud has increased: 83%

Areas of High Vulnerability: Information theft, loss or attack (26% of sector firms indicate that they are highly vulnerable) • Management conflict of interest (18%)

Areas of Frequent Loss: Regulatory or compliance breach (29% have experienced in past three years) Internal financial fraud or theft (28%) • Information theft, loss or attack (27%) • Theft of physical assets or stock (26%) • Financial mismanagement (23%) • Management conflict of interest (23%)



CASE STUDY

OPERATION MALAYA: Corruption in the Spanish real estate sector

Since the beginning of the 1990s, Spain's "economic miracle" has brought an exponential increase in investment in coastal areas. Marbella, the world famous tourist resort of the international jet set, has seen money, mostly foreign, pour into real estate. Sumptuous villas have appeared, accompanied by the rapid, disorderly spread of houses, apartments and commercial centers.

The frantic activity of real estate promoters, backed by flexible and inventive banks, has driven growth by allowing Spaniards to think that they were making safe investments. Speculators, however, helped by inadequate regulation, brought with them money laundering, corruption, coastal and environmental devastation and exploitation of limited natural resources such as water to build golf resorts.

The Importance of Due Diligence

In this context, an important foreign institutional investor asked Kroll to assist him in a due diligence study of certain major construction companies in the region with which he hoped to form an ongoing relationship. We found, mainly through documentary analysis, that some of these firms did not have a clear background – incomplete accounts, overly rapid growth, lack of long-term personnel – and that some were too close to local politicians. We concluded that there was a serious risk that these companies might be involved in improper business practices, and advised our client accordingly.

The biggest difficulty was explaining to our client why our findings were sufficient to cause him concerns regarding his investment. He wanted hard evidence, while we had strong indicators. Our professionals met with the client and eventually he understood our position.

In March 2006, less than one month after we delivered the report to our client, Operation Malaya made national and international headlines. After a year-long investigation, police arrested most of Marbella's city government on charges of corruption, money laundering, and several other offenses. The operation continued in other Spanish regions, including most of the South, Madrid and the Basque Country. As a result, 86 people are undergoing trial, among them the



executives and owners of some of the companies with which our client had wanted to work. Following our report, our client was able to find other partners and his only loss was a few months' time. Without the due diligence study, he would probably now be trying to explain to a judge and to the press his presence as a shareholder of some of the indicted businesses.

The Mechanism: Land Rezoning

Operation Malaya exposed the fraud risks that can be involved in the real estate sector when certain conditions are present. A generally positive perception of real estate development – along with a lack of clear rules and scrutiny – allowed politicians and developers to illicitly split the gains from real estate sales in exchange for construction licenses and rezonings of protected land. Construction firms paid huge amounts to politicians, knowing that an extraordinarily receptive market would pay any price for houses, commercial centers and resorts. To make things run smoothly, all such arrangements were handled through one of the Town Hall's advisors, who was in complete control of real estate operations in Marbella. Although citizens suspected corruption existed, the magnitude of the scheme once fully exposed left indignation and bewilderment.

Due diligence, even if it does not produce a smoking gun, can make clear which companies to avoid and why.



Alessandro Nurnberg is a senior director in Madrid specializing in investigations into offshore structures. He previously worked as a tax and legal advisor for TS Group in Lugano, Switzerland and later advised clients on M&A, public sale offers and fiscal offshore structures at Ernst & Young.

EIU SURVEY

Corporate fraud at financial services companies is a very expensive problem. The particular forms that it takes result from three features of the sector: that it deals with money itself; that this is held largely in an electronic form; and that sector activities are closely regulated.

- The loss per firm is \$14.6m, well over twice the average for all industries and the highest in our survey.
- Increasingly complex information technology has left 43% of respondents more exposed to risk. Consequently 27% have suffered from information theft in the past three years, and 28% consider themselves highly vulnerable to this most widespread worry for the sector.
- In practice, regulatory and compliance breaches make up the most common problem, having affected 29% of companies. This risk represents an area of high vulnerability for 17% of respondents.
- Money laundering is understandably a particular problem in financial services, although less common than the others discussed. More than one in ten firms consider themselves highly vulnerable to it and a similar number have actually suffered from it in the past three years. Given the attention that governments, regulators and security agencies pay to illicit cash flows in the post 9/11 world, these figures are far too high. Failure here will attract little sympathy or leniency.
- Internal financial fraud is significantly more common, hitting more than one-quarter of firms, but theft of physical property is rarely a problem. The asset worth stealing in this industry is money rather than stationary.

The sector is working harder than most to combat corporate fraud, but could do more.

- The use of most anti-fraud strategies is far more widespread within financial services than among other businesses. For example, 85% use financial controls to combat such problems (compared with an average of 79%); 80% use IT security measures (compared with 70%); and 69% use staff background screening (compared with 57%).
- Formal risk management systems are more than one-and-a-half times more common in this sector than overall.
- Financial services companies are much more likely to plan to invest in financial controls, IT security and management controls to combat fraud than their counterparts in other sectors.
- However, although 85% of firms use financial controls against fraud, this means that nearly one in six financial services firms do not. In this industry, such arrangements should be second nature, and would help with some of the biggest vulnerabilities.

The financial services industry is working much harder than most but, given the financial and legal costs of failure, it needs to do even more.

Written by The Economist Intelligence Unit

Private equity, hedge funds and emerging markets: Playing risk for returns

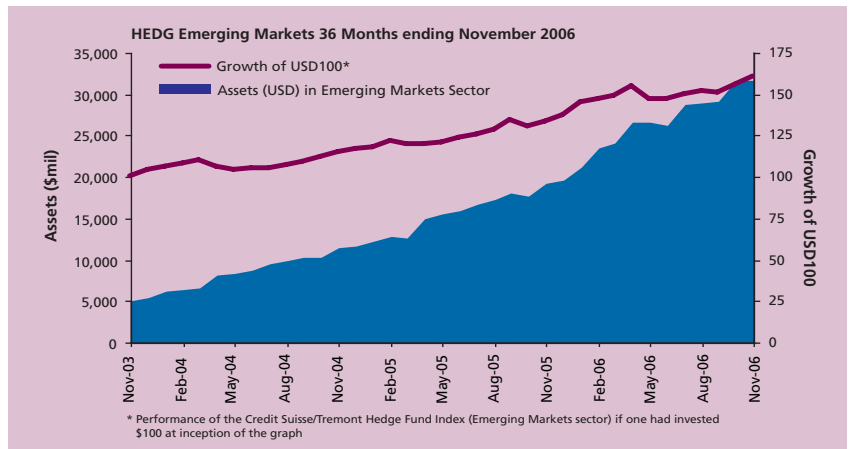
You cannot pick up a newspaper today without seeing an article that discusses a new hedge fund, a new investment strategy, incredible returns, and the successful bets against the market that have made an unknown manager famous. Around the world, hedge funds are seeing tremendous capital inflows: In Q1 2007 these totaled an estimated \$60 billion, four times the figure for Q4 2006.¹ Total assets now are usually estimated at around \$2 trillion, with some putting the figure as high as \$3.5 trillion.

The attraction is simple: Historical returns for hedge funds have bested nearly every other investment opportunity. The news from emerging markets is even better: Returns in Q2 2007 averaged around 9.7% according to Morningstar, Inc., and in recent years such investments have seen 20% growth. Consequently, hedge funds focused on emerging markets have exploded from \$2.6 billion in assets under management in 2003 to nearly \$32 billion by late 2006, according to a recent Credit Suisse report (Chart 1).

Such performance has attracted a broad array of investors including endowments and state pension funds. Endowments and state pension funds continue to expand their holdings into hedge funds and alternative investments in emerging markets. By March 2006, the California Public Employee Retirement System had invested more than \$300 million in a variety of Asian hedge funds, and in the

A few simple questions may help protect the investor from fraud:

- Was the investor introduced to the manager/investment opportunity through trusted sources?
- Does it all sound too good to be true?
- What impressions did the investor get when meeting with the hedge fund management team?
- Were they candid and helpful?
- Who are the third party service providers for the fund – lawyers, accountants, back office administrators? Are they reputable? Can they provide independent confirmation?
- Who is the fund manager?
- What are his or her credentials?



Credit Suisse Tremont Hedge Fund Index, January 2007

past year the University of Texas, Harvard University, and other schools have announced plans to increase their allocations in emerging market funds.

The performance has also, however, compounded risk: An increasingly large number of funds flush with capital are competing over a limited number of investments. A larger number are very young and headed by managers with little to no track record. Low barriers to entry and low thresholds of regulatory oversight continue to allow new funds to proliferate. Many are small – over half have fewer than 10 employees – and depend heavily on only a few people for their performance, driving up operational risks.

More problematic still, although China, India, and Brazil still draw interest, the race to keep returns high has pushed some funds into riskier investments in “new emerging markets” such as Colombia, Angola, Vietnam, and Mongolia. Investors in these markets have to be prepared to guard against corruption and unpredictable political and economic climates. Those buying into the funds, however, may have little knowledge of where their money is going.

While the news is dominated with stories of the collapse of large scale funds, a host of lesser known ones are closing in emerging markets. Some have made bad investments. Others have fallen victim to outright fraud. In 2005, the Aman Capital Global Fund, once the flagship of Singapore’s hedge fund industry, collapsed after only one and half years when it lost an estimated 18% of its assets on derivative trading on the Korea

Composite Stock Price Index. While its managers were highly regarded, investors questioned the soundness of the fund’s internal risk controls. Last year, Charles Schmitt, the Hong Kong-based head of the CSA Absolute Return Fund, was sentenced to four and half years in prison for channeling over \$190 million from investors into shell companies administered on his behalf, some of which were used to pay his personal expenses, which included a Hawaiian home.

Funds investing in emerging markets require extra due diligence. Investors, particularly institutional ones, must undertake responsible efforts to understand with whom they are doing business and the types of investments being made. With the amount of capital such institutional investors bring to the table, they are in a unique position to pressure fund managers for additional transparency and information about the fund’s operations, performance, and risk controls.

Adequate due diligence is a cost of doing business in any market, especially an emerging one, and should be viewed as part of the investment, not a sunk cost. It is certainly cheaper than undertaking litigation, chasing assets, and repairing reputations after a failed investment.

¹ Hedge Fund Research Inc.

Peter Turecek is a managing director in New York. He specializes in hedge fund related intelligence, corporate contests and securities fraud.

Julian Grijns is an associate managing director in New York. He previously worked at Towers Perrin in their competitive intelligence program.

ALTERNATIVE SECURITIES: Opportunity for fraud and reward

The collapse of the sub-prime mortgage market has rekindled a debate about the economic impact of fraud in the insatiable markets for high yield alternative investments. Did the fraudulent practices of a few originators and issuers of these mortgages spark the downfall of the market, or was it due to cyclical economic forces? Watchdog organizations often spend years after the fact trying to find the answer. Investors should ask a more important question: could the potential fraud have been identified in advance and therefore avoided?

Just like any stock-picker or analyst, fraudsters follow the market, recognizing a hot market as a ripe one. Fast-paced capital markets are always creating new investments, providing fertile ground for modern-day Charles Ponzis to develop schemes that are more complicated and take longer to unravel. At first glance, the neo-fraudster might seem to be using new and exotic investment vehicles and methods in order to bilk investors, but a closer look usually reveals a simple daisy chain or Ponzi scheme.

Two trendy investments are life settlement-backed securities and alternative energy. There are regular media reports about fraud in these markets, although the underlying economics are sound. Appropriate diligence can separate the scams from the true opportunities.

Death Bonds

A recent *Business Week* cover story reported that in May more than 600 Wall Street bankers “gathered at a conference in New York to talk about the next exotic investment coming down the pike: death bonds,” now called life settlement-backed securities.

Is this a resurgence of the discredited viatical market, which emerged in the 1990s in the wake of the AIDS epidemic? Sellers, typically the elderly or terminally ill, sold the right to their eventual life insurance policy death benefits for an up front payment. Bundled viatical policies were marketed as securities to individual investors.

The industry has changed and aging baby-boomers have fueled a “bustling market” for unrated Death Bonds, which first emerged in Europe and now are hot in the United States, according to *Business Week*. This market, however, has attracted its share of fraudsters, and regulators have reissued warnings about illegal and unethical practices:

- A 2004 Kroll due diligence investigation of a viatical firm revealed that its founder had formed the company solely to take advantage of a hot market. His previous two businesses, in distinctly different industries, left a trail of litigation and he had previously sought personal bankruptcy protection.
- From the mid 1990s until 2004, Mutual Benefit Corp., a Florida-based life settlement company, bilked 30,000 investors out of \$830 million. In 2004, the Securities and Exchange Commission sued to shut it down. In 2007, its executives were convicted of federal crimes and the company, now in receivership, pleaded guilty to racketeering and investment fraud charges.

Alternative Energy Investments

With oil prices close to all-time highs, the traditional and alternative energy markets are booming, and so are investment scams. Investors looking for a quick return are losing millions of dollars in sham oil and gas investments. In January 2007, the North American Securities Administrators Association reported that, over the preceding two years, state and provincial regulators had opened more than 260 cases involving oil and gas-related schemes and issued 122 cease and desist orders against promoters. In particular, a flood of investments into companies with “new” technologies that have no industry expertise harks back to the dot.com boom and bust of the 1990s.

Appropriate diligence can separate the scams from the true opportunities.

The alternative energy market has even seen a scam involving an entirely phony exchange. In May 2007, a federal judge entered a default judgment against American Energy Exchange and York Commodities after the U.S. Commodity Futures Trading Commission charged them with fraudulently soliciting customers to trade non-existent energy futures on a non-existent exchange through a fraudulent broker.

Fraud also appears on legitimate exchanges. In April 2007, the *Financial Times* reported on “widespread failings in the new

Seven red flags

- The company had no track record, and the principals had no real experience in the industry;
- The business operated in an essentially unregulated industry or was able to skirt weak or newly emerging regulation;
- The principals provided resumés that were lacking in detail and, upon investigation, proved to be inaccurate;
- The principals did not provide adequate information on, let alone audited statements of, the financial performance of their current or past ventures;
- The investment involved a needlessly complicated corporate structure and the principals controlled multiple shell or related party companies;
- The principals were reluctant to share information about their current or past business partners;
- The principals, their previous partners, or their companies had been subjects of significant civil and criminal litigation, and had numerous liens or judgments.

markets for greenhouse gases, suggesting some organizations are paying for emissions reductions that do not take place.” Among other things, it found organizations buying “worthless” credits, industrial companies profiting from doing “very little” and brokers providing “questionable” services.

History: An Investor's Guide

Market history and lessons learned from due diligence can reveal potential fraud in advance and may help predict the strength of a particular security or market. Just as an actuarial or bond rating house uses empirical data to predict the quality of an investment, a due diligence investigation of the persons involved and their record allows investors to understand the potential risks.

Michael Fellner is a senior managing director and head of the Chicago office. He specializes in corporate contests, embezzlement and political corruption and bankruptcy fraud cases. Previously he worked as a journalist and ran his own investigations agency.

Lisa Silverman is a managing director based in Chicago. She specializes in investigative cases for corporate contests, theft of trade secrets, patent infringement and product tampering.

Mark Skertic is a director based in Chicago. Prior to that he worked for over 20 years as an award winning investigative journalist at the *Cincinnati Enquirer*, *Chicago Sun-Times* and the *Chicago Tribune*.

EIU SURVEY

The professional services industry has a low exposure to fraud relative to other sectors

- The loss per firm for the past three years is \$2.3m. This is equivalent to around one-third of the survey average and is one of the lower figures.
- Respondents believe that the prevalence of fraud has stayed the same over that period.
- Fewer professional services firms have experienced each category of corporate fraud than the average, except for information and IP theft. In particular, only 20% suffered from theft of physical assets. Although this arises partly from the sector being knowledge-intensive without a physical product, the figure is still the lowest for any industry.

This sector includes professions that actively combat fraud, or for which suspicion of fraud presents an increased danger because reputation is so important in maintaining clients. This has several effects on the nature of, and response to, corporate fraud.

- These companies are more likely to deal with the issue directly and combat the problem themselves. Sixty-one percent say that they manage it in house compared with 45% of all companies.
- Accordingly, professional services firms are half as likely to turn to the big four accountancy firms (16% compared with 33% for the average).
- In the past three years, a slightly lower percentage of companies than average has suffered from bribery and corruption (15% compared with 19%), regulatory breaches (15% compared with 19%) and money laundering (2% compared with 5%)

The sector faces the usual problems of a knowledge industry, but may not be addressing them aggressively enough.

- The most frequently reported types of fraud are information theft (29%) and IP theft (21%). These are also two of the three areas where the greatest number of respondents feels highly vulnerable (26% and 19% respectively).
- Complex IT structures have increased exposure to fraud at one-third of companies.
- However, the proportion of companies using IT security and countermeasures to combat fraud is only 69% and just 57% say that they intend to increase investment in that area. Both of these figures are slightly lower than the average. Meanwhile, only one-third of professional services firms say that they engage in IP monitoring – this is lower than the average – and just 37% are looking to invest in this area.

The professional services sector should pay particular attention to IT security and IP monitoring, especially as legal and accounting firms should already be strong in other aspects of fraud control.

Written by The Economist Intelligence Unit

Preventing risk in the people business

From one side of Kroll's London offices, one has a splendid view of St Paul's Cathedral. From another, there is a vista of Fleet Street, long the home of the British press; and from a third, the harsh lines of the Old Bailey, London's Central Criminal Court.

If management ever needs a reminder of the risks faced by the modern professional services firm, a swift walk around the building should suffice. Reputational, ethical and legal issues abound. The central issue, for professional services firms, is about governance: getting everyone to address the issues systematically and globally, to link together diverse functions (financial, legal, HR), and above all to get billable professionals to devote scarce and valuable time to risk prevention.

Like many professional services firms, Kroll has offices around the world with diverse cultural backgrounds, histories and legal frameworks, and getting a common approach is a challenge. The solutions tend to lie in pragmatic answers: working with the grain of the business and getting each office and region involved. Legal, risk and compliance functions need to co-operate. Standard operating procedures need to be clear, but also simple enough to adapt to a wide variety of operating environments.

Many such companies are made up of individuals who either are, or operate as, partners: they own the business, and that can be a great strength, conferring a sense of responsibility and focus. But at the same time, it can make the business harder to navigate: people are jealous of client relationships, reluctant to discuss "their" business, and ill-disposed to efforts to



centralize or co-ordinate risk management. The only answer is to treat individuals as individuals, and get buy in – while also leading from the top, to ensure that everyone knows that rules are rules.

These are people businesses, so management of human capital is critical. Professional qualifications and licensing are important, which means ensuring that background screening is carried out and that staff references are taken up. Conflict checking systems are essential – but so is the training and education that enables people to understand how to operate them, and how to make sensitive judgments about what constitutes a conflict and how to handle it.

A critical issue for professional services firms is the vetting of projects before they are taken on. Kroll, like many such firms, has regional risk committees that review projects assessing whether legal, reputational and financial issues are in line with the law, standard operating procedures, and our business model.

Andrew Marshall is a managing director based in London and Washington, having previously held the roles of chief risk officer and head of strategy EMEA. He spent 15 years as a journalist including serving as Foreign Editor and Washington Bureau Chief for *The Independent* newspaper.

REPORT CARD PROFESSIONAL SERVICES

Financial Loss: Average loss per company over past three years: U.S.\$2.3m (34% of average)

Prevalence: Percentage of companies suffering corporate fraud loss over past three years: 83%

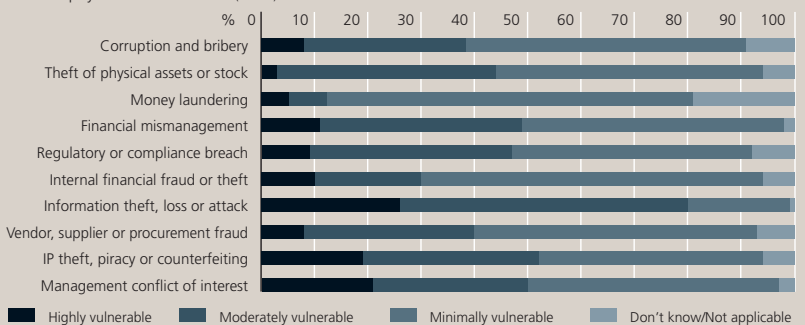
Increase in Exposure: Percentage of companies where exposure to fraud has increased: 89%

Areas of High Vulnerability: Information theft, loss or attack (26% of sector firms indicate that they are highly vulnerable to this threat) • Management conflict of interest (21%)

Areas of Frequent Loss: Information theft, loss or attack (29% have experienced in past three years)

IP theft, piracy or counterfeiting (21%) • Management conflict of interest (21%)

Theft of physical assets or stock (20%)



Procurement data can help fight fraud

Internal audit managers can increasingly rely on the data in procurement systems to analyze the behavior of staff. E-procurement tools let organizations see not just how much a department is spending with a supplier, but what is being bought by individual staff members. Most procurement departments use this data to analyze contract compliance and the opportunity for greater savings, but it can also be used to detect fraudulent transactions before they occur.

Some advisors still suggest that companies can detect fraud if they monitor their staff for signs of sudden affluence. While this may be a sound signifier for fraudulent activity, it is hardly a reliable method of detection. Monitoring spend activity is the best opportunity that organizations have of identifying staff who process fraudulent transactions. In most cases, this activity is predictable and, if managers establish a service to monitor buyers, much of it can be identified before any payment is made. In large international organizations, where thousands of orders can be raised per day, it is not feasible to monitor every transaction, but they can be profiled in order to flag those that carry the highest risk of fraud.

Profiling can help identify the types of buyer most likely to commit fraud and combine this with the transactions most likely to attract it. For example, a temporary staff member raising a high value order should be seen as high risk. Similarly, the purchase of desirable consumer goods, such as audio-visual equipment or alcohol, should be flagged as high risk. Individual buyers can be put "on probation", their activity monitored and transactions flagged according to different levels of security risk.

Very high risk transactions can be sent for re-approval by departmental managers or investigated by audit managers before being processed. This additional step serves a dual purpose: as well as identifying fraud, it can act as a deterrent by showing that a buyer's activities are being monitored.

Our extensive experience in fraud investigations suggests that the following is a reliable guide to setting up a transaction profiling service:

Do:

- Test the profile and monitor the volume of flagged transactions;
- Provide clear communication to buyers about why a transaction has been flagged;
- Handle investigations or re-approvals quickly and efficiently;
- Update profiles if buyer circumstances and departmental needs change;
- Review profiles annually in order to ensure they are effective;
- View profiling activity as a long-term commitment.

Don't:

- Infer that buyers are acting fraudulently before investigating the transaction;
- Assume that a profiling service will capture all fraudulent transactions;
- Transgress any equal opportunities legislation when profiling buyers;
- Allow buyers to be aware that they are or are not being monitored: they should assume that they always are.

Ticon provides consulting and research services for public and private sector organizations. It specializes in services for organizations who want to improve their procurement and supply chain management through the use of e-procurement.

EIU SURVEY

Manufacturers as a whole are less worried than those in other sectors about corporate fraud.

- The figures for perceived vulnerability to corporate fraud within this sector are generally about the same as the overall average, although in some instances they are slightly lower. Only in one area, procurement fraud, is vulnerability perceived to be higher than average.
- Spending on the leading anti-fraud strategies is also less widespread in this field than among the overall survey respondents, especially for IT measures (used at 59% of manufacturers against 70% overall), management controls (54% to 64%) and staff screening (48% to 57%). Future investment in these fields also looks set to lag behind that by other sectors.

In practice, however, little reason exists for complacency.

- Manufacturers have experienced higher than average incidences of several types of fraud, including: theft of physical assets (47% compared with 34% for the overall sample), corruption and bribery (28% compared with 19%), financial mismanagement (26% compared with 20%) and intellectual property theft or counterfeiting (23% compared with 13%).

- The loss per firm for this sector is slightly above average, as is the proportion of firms suffering from at least one form of fraud in the past three years.

- The growth in exposure to fraud is hitting more companies in this industry than on average (88% compared with 81%). The necessities of globalized competition mean that entry into new markets, IT complexity and increasing collaboration between businesses are all increasing the risk of fraud at a faster rate than elsewhere.

Manufacturing companies need to understand better the degree of risk they face, and to invest accordingly.

Written by The Economist Intelligence Unit

REPORT CARD MANUFACTURING

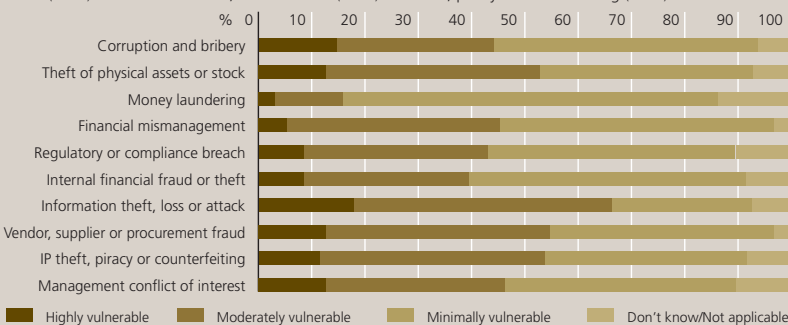
Financial Loss: Average loss per company over past three years: U.S.\$6.8m (101% of average)

Prevalence: Percentage of companies suffering corporate fraud loss over past three years: 88%

Increase in Exposure: Percentage of companies where exposure to fraud has increased: 88%

Areas of High Vulnerability: Information theft, loss or attack (18% of sector firms indicate that they are highly vulnerable) • Corruption and bribery (15%)

Areas of Frequent Loss: Theft of physical assets or stock (47% have experienced in past three years) • Corruption and bribery (28%) • Financial mismanagement (26%) • Vendor, supplier or procurement fraud (25%) • Information theft, loss or attack (23%) • IP theft, piracy or counterfeiting (23%)





Hijacking pharmaceutical brands: A study

In June 2007, MarkMonitor undertook an in-depth study of the online hijacking of popular pharmaceutical drug brands, including millions of emails and billions of Web pages. It focused on six popular prescription drugs – three of the most popular drug brands, according to industry reports, and three of the drugs most searched-for on popular search engines – and identified over 3,100 Internet pharmacies selling one or more of these, along with 390 individual listings on bulk exchange sites.

The key findings of the study include:

Business practices at many online pharmacies are spotty. Traffic intended for legitimate websites is diverted to suspicious ones, diluting overall brand and marketing efforts. Many of these pharmacies fake their accreditation deliberately, so it is almost impossible for a visitor to know their provenance. The recent death of a Canadian woman who ingested questionable drugs purchased online shows the dangers of not shopping at an accredited drugstore.¹

There are strong indications that the drugs supplied are not genuine. One-tenth of the sites require no prescription, and only four out of more than 3,000 sites have Verified Internet Pharmacy Practice Site (VIPPS) accreditation. More worrying still, average prices for medications are about a fifth of those charged by the certified sites.

Online pharmacies endanger consumers' identity information as well as their health. The majority of the servers hosting these websites do not protect customer transaction data with Secure Socket Layer encryption, and more than 20% of the post-purchase email analyzed in the study contained links to unauthorized customer data.

The problem extends to drug exchanges and drug distribution channels. Twenty-one of the 390 individual listings studied on these bulk exchange sites offered deeply discounted prices that raise questions about product integrity. China was the primary source of these listings (31%), followed by India (19%). This activity poses a serious risk to the overall drug supply chain, compromising product delivery by putting phony or dangerous medications into the retail network.

¹ <http://www.medicalnewstoday.com/articles/76431.php>

MarkMonitor® is in the business of protecting enterprise brands online, helping strong corporate reputations become even stronger in the digital world. It can help the world's largest companies establish brands online and help them combat the growing threats of online fraud, brand abuse and unauthorized channels. Over half of the Fortune 100 trust MarkMonitor for online brand protection and Internet fraud prevention. www.markmonitor.com

REPORT CARD HEALTHCARE, PHARMACEUTICALS AND BIOTECHNOLOGY

Financial Loss: Average loss per company over past three years: U.S.\$11.7m (175% of average)

Prevalence: Percentage of companies suffering corporate fraud loss over past three years: 82%

Increase in Exposure: Percentage of companies where exposure to fraud has increased: 81%

Areas of High Vulnerability: IP theft, piracy or counterfeiting (25% of sector firms indicate that they are highly vulnerable to this threat) • Information theft, loss or attack (24%) • Regulatory or compliance breach (21%)

Areas of Frequent Loss: Regulatory or compliance breach (31% have experienced in past three years)

Theft of physical assets or stock (25%) • Financial mismanagement (25%) • IP theft, piracy or counterfeiting (22%) • Management conflict of interest (22%)



Counterfeiting in the pharmaceutical industry: Ten pieces of advice

The production and sale of counterfeit drugs is much more attractive than that of many other products for a variety of reasons: costs can be considerably reduced if cheaper substances, often not even pharmacologically active, are used; no large facilities or sophisticated plants are required as manufacturing can take place in a back yard; cheap or slave labor can be employed; and producers do not have to engage in complex R&D. What makes counterfeit drugs most attractive and keeps gross margins up is the ample and elastic market they enjoy.

This market takes different forms around the world, but is always there. According to the World Health Organization, "in wealthier countries, the most frequently counterfeited medicines recently have been cholesterol lowering medicines, drugs used for treatment of growth hormone deficiency and for cancer. In developing countries the most counterfeited medicines are those used to treat life-threatening conditions such as malaria, tuberculosis and HIV/AIDS. ... However, there are variations that encourage specific types of counterfeit medicine, depending on the geography, climate and seasonality inherent to each country."¹

Intellectual property fraud against pharmaceutical companies not only results in lost market share, but strongly impacts public health and the brands of targeted firms. The following ten pieces of advice distill lessons Kroll has learned in helping clients minimize losses from this fraud.

1. Apply good manufacturing practices rigorously: Security standards along each step of the manufacturing chain must be strictly enforced. Periodic reviews, sample testing, simple policies such as "clean desks", familiarity with business partners, strict inventory controls, and formal logistics processes all help reduce potential losses.

2. Use distinctive packaging: Although counterfeiters will seek ways to copy drug packaging, mechanisms to differentiate products and security items – hologram seals, embossing, security codes, self-destructing seals, scrape-off inks, and different tagging and tracking systems – make it much more difficult for them.

3. Report instances of counterfeit drugs: A database created by the whole industry will enable mapping of the appearance of such drugs and help investigative agencies to identify counterfeiters. Because many of the substances used to manufacture these products are imported, the industry must extend its efforts globally, beyond the country where the drugs are made or sold.

4. Control invoices: There are cases where manufacturer invoices are also faked, adding credibility to the counterfeit drugs and

making the job of law enforcement agents harder. Controlling the invoice printing process, using specific forms that include security items, and electronic invoicing help inhibit such practices.

5. Monitor product and scrap disposal: Drugs are perishable and, as such, the recovery and handling of expired products should be an intensely audited effort. The same is true for products returned for different reasons, even those of quality. Production leftovers and obsolete equipment should be destroyed under the supervision of the management and control group.

6. Make hotline systems a part of consumer services: Putting these two systems together creates a lot of information that investigators can use. Mapping the areas most affected by counterfeiters will only be effective if the information collected is ample disseminated using these channels.

7. Study the enemy: The Internet is an increasingly important mechanism to reach out to consumers. Counterfeiters have known this for a long time. Watching their sales activity through use of a reverse chain can help establish their distribution logistics. Search filters, search engines, specific search clippings, statistical survey modeling, and data mining are effective Internet monitoring tools.

8. Periodically review the processes involved in product creation and development: Project drafts, notes on pieces of paper, formula matrices, as well as photoliths printed without proper control can all be of great value to counterfeiters.

9. Train and retrain: Programs developed by security auditors and managers should be broadly disseminated within the organization and periodically reviewed to inculcate a culture of security.

10. Promote teamwork: When staff from marketing, information technology, sales, legal, finance, operations, and institutional relations get together and share information, coordinated by an integrated intelligence center, success against fraud improves dramatically.

By doing the above, pharmaceutical firms can go a long way to shielding themselves from the threat of counterfeiters, thereby protecting public health and their own intellectual property.

¹ WHO Drug Information Vol 20, No. 1, 2006



Vander Giordano is a managing director based in Miami 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

Corporate fraud is a particularly serious issue for this sector

- The loss per company over the past three years has been \$11.7m, more than 75% above the average.
- Among the industries questioned for this survey, healthcare, pharmaceuticals and biotechnology are among the most likely to expect an increase in prevalence of fraud, with 40% reporting growth and only 28% pointing to a decline.
- Companies in this sector are more likely than the average to feel highly vulnerable to every type of corporate fraud risk, with the exception of money-laundering.

As a highly regulated knowledge industry, areas related to data and government relations pose the biggest concerns.

- The areas where firms are most likely to feel highly vulnerable are IP theft (25%), information loss (24%), compliance breaches (21%) and corruption (18%).
- Complexity of IT is the most common cause for increased exposure to corporate fraud in this industry. It is cited by 41% of respondents.

Actual losses show a mixed picture, including that more work is needed in the areas of IP protection and compliance.

- The sector has not suffered unduly from information theft and corruption. Twenty-two percent have experienced the former during the past three years, compared with 20% for the overall sample, and 8% have experienced the latter, which is again lower than the average of 19%.
- In contrast, 31% have experienced regulatory or compliance breaches (compared with an overall average of 19%) and 22% have experienced IP theft (compared with 13% for the average).
- Less than half of companies in this sector engage in IP monitoring and only one-third intends to invest in starting or improving such programmes.

This sector has been able to do very well in certain key areas, but needs to address specific weaknesses, notably compliance and intellectual property.

Written by The Economist Intelligence Unit



Machinations in the Japanese entertainment industry

Off-the-book money remains as important as ever in Japan's entertainment industry, and methods for facilitating such payments have become an established part of business models for many companies. Cash and personal relationships are all-important in this world, where under-the-table payments are not always regarded as a vice. The result is that many companies have extremely lax internal controls, with practices such as payment in cash to avoid income tax or executives having several companies with opaque activities.¹

The case of Alpha Video helps to demonstrate the extent of such activity and the difficulties in stopping it. The company was launched in Japan some fifteen years ago and subsequently purchased by the European firm Beta. Alpha's operations

were limited for some time, but suddenly picked up five years ago, following the appointment of Akira Z as CEO. Z embarked on a series of new projects outside the company's main field of videos and adopted a strategy to raise Alpha's brand profile. In cooperation with external funders, he embarked on capital reinforcement and strengthening management.

Z's initiatives led to cost overruns, unaccounted payments, and the reassignment of accounts, which led Beta to intervene vigorously. Since the CEO was highly regarded by his staff and the market, these attempts to improve controls did not go smoothly. However, Beta discovered a case of account-rigging carried out two years before Beta had purchased Alpha, and the company was shocked into action.

An in-house investigation found that Z had without Board approval carried out a window-dressing fraud (where accounts are manipulated so that revenue is booked before year-end but later reversed) using a listed Japanese company. In the year in question, the company had suffered major losses on video sales. Z arranged to sell to a business called Japan Video, the representative of which was an old friend, several hundred videos with content of no commercial value for ¥300 million. Japan Video had no plans to use the merchandise, which remained in Alpha's warehouse. Originally, the plan had been for Japan Video to sell back the videos for the same amount at the end of its financial year, but instead the company ostensibly sold Alpha a variety of projects for a total value of ¥300m over a year's period. Those involved denied absolutely that these sales were part of an exchange because of the impact that the window-dressing might have had on Japan Video's reputation as a listed company.

Other examples of kickbacks and shell companies to hide illegal payments later came to light, although these were for the personal benefit of the management rather than for that of the business. An investigation by Kroll showed that both the legal and financial departments had issued repeated warnings. A senior legal officer who had discovered what was going on made a direct appeal to a higher authority and – in a quintessentially Japanese outcome – was himself forced to resign. These efforts bore no fruit in a company that kept no proper records, even of Board decisions. Only the arrival of Beta led to a review of corporate governance and the hiring of Kroll.

It need not be this way. Data from the United States suggests that the entertainment industry does not have a particularly high rate of improper activity in comparison with others. In Japan, however, the tactics used are overt and senior executives need to increase their awareness of the magnitude of the effects that fraudulent activities may be having on corporate governance.

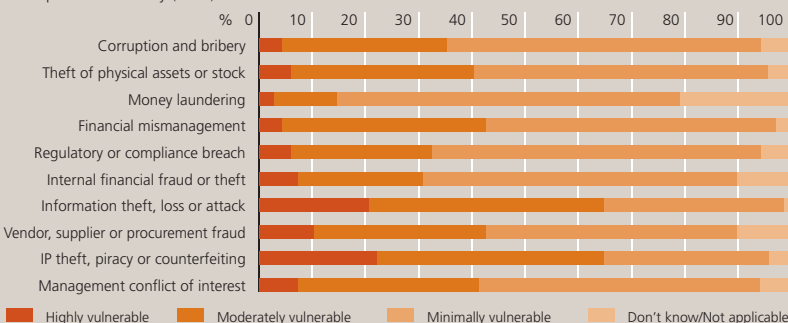
¹ All the names and significant details have been altered in this account, to prevent identification of the case.



Tsuyoki Sato is a managing director and director of operations in Tokyo where he has carried out fraud investigations in industries including entertainment, IT and manufacturing. He is a member of the Association of Certified Fraud Examiners (ACFE) and the American Society of Industrial Security (ASIS). He previously worked as an investigative reporter.

REPORT CARD TECHNOLOGY, MEDIA AND TELECOMS

- Financial Loss:** Average loss per company over past three years: U.S.\$4.9m (63% of average)
- Prevalence:** Percentage of companies suffering corporate fraud loss over past three years: 77%
- Increase in Exposure:** Percentage of companies where exposure to fraud has increased: 88%
- Areas of High Vulnerability:** IP theft, piracy or counterfeiting (22% of sector firms indicate that they are highly vulnerable to this threat) • Information theft, loss or attack (21%)
- Areas of Frequent Loss:** Theft of physical assets or stock (28% have experienced in past three years) Information theft, loss or attack (27%) • Vendor, supplier or procurement fraud (24%) Corruption and bribery (21%)



CASE STUDY

Old-fashioned fraud: A case study from China

In 2000 the managing director of a technology, media, and telecom subsidiary of one of Asia's biggest conglomerates was introduced to Mr. X, president of a group of Californian companies. Mr. X spoke with passion about new technologies his businesses had developed that would revolutionize the delivery of cable television. A limitless choice of content would be available at the touch of a button with no download delays. Moreover, the system was inexpensive and required minimal bandwidth.

Mr. X persuaded the conglomerate to invest in shares of his companies and to purchase pilots of the system. In return, it received exclusive rights to commercialize Mr. X's system across China. As the project progressed, Mr. X repeatedly requested more money, claiming each time that his researchers were on the brink of significant breakthroughs and that the additional funds were required to get them across the line. From time to time, he took huge bonus payments, explaining that he was using them to pay scores of consultants who were involved in the project "behind the scenes."

After several years and more than U.S.\$700 million, the Asian conglomerate accepted the painful reality that it had received nothing of value – just incomplete parts of an expensive, substandard system – and that it never would. It commenced legal proceedings in California against Mr. X and his companies and had the latter's accounts effectively frozen. By now it was suspicious that a British Virgin Islands company, which Mr. X had described as an independent, third-party supplier, was in fact controlled by him or associates. Mr. X's companies had purchased large quantities of memory modules from this firm and resold them to the Asian conglomerate. The suspicion was that the BVI company had purchased the memory modules from a genuine supplier and then sold them to Mr. X's group at highly inflated prices; its involvement had been required simply to hide huge mark-ups from the final purchaser.



The conglomerate had the Californian court issue a letter of request to a court in Hong Kong seeking production of documents relating to the BVI company's bank accounts there. The Californian group and the BVI firm resisted all the way to the Hong Kong Court of Appeal.

A "director" of the BVI company listed a Tokyo address in an affidavit: on checking, it turned out that the address was that of a public car park. He also gave an office address in Shanghai, which proved not to exist at all.

With the aid of the Hong Kong courts, the Asian conglomerate finally obtained the bank records. These showed that Mr. X's mother and brother controlled the BVI company's accounts. Mr. X's defense in the Californian

proceedings collapsed, as did those of his companies. The conglomerate obtained a judgment for U.S.\$2.8 billion (including U.S.\$2 billion in punitive damages).

The case highlights the importance of conducting thorough due diligence on new business partners and technologies. Although it is not what happened here, some businesses are blind to the investment risks when faced with the vast China market and its opportunities. On the more positive side, the case also shows that a coordinated effort by a multi-jurisdictional team of lawyers and investigators can achieve significant recoveries even when pursuing a sophisticated fraudster. The courts in many jurisdictions will be eager to assist and this case should, in particular, give reassurance to Asian companies seeking to pursue U.S. companies through the American courts.

ORRICK is an international law firm with approximately 980 lawyers located throughout the United States, Europe and Asia. The firm traces its roots back to 1863 and since that time, it has expanded its practice groups and extended its global reach with one core strategy in mind: focusing on solutions and results in response to its clients' current and future needs. Its size, resources, geographic breadth, advanced IT systems and business-oriented culture ensure that its clients receive responsive, value-added services.



EIU SURVEY

As a knowledge industry, this sector is more concerned about information theft and IP issues than most, but is much less focused on other corporate fraud issues.

- The areas of most common concern are IP and information theft. More than one in five respondents consider themselves highly vulnerable in these areas.
- Complex IT structures have increased exposure to corporate fraud at 35% of businesses within this sector.
- Accordingly, IT security is the leading area for investment – it is currently used by 57% of companies. In addition, IP monitoring is much more common than average (52% compared with 36%). These companies are also much more likely to have their legal department lead efforts against fraud (22% take this approach, compared with 13% among all respondents).

The record suggests that the level of concern companies are showing is justified.

- The loss per business in this sector from corporate fraud is less than two-thirds of the average.
- Physical theft of assets, which is the most widespread problem in this sector, financial mismanagement and management conflict of interest are all less common than average.
- Although the number of firms hit by IP and information theft in the past three years is slightly higher than average, the differences are not dramatic. Nineteen percent have experienced IP theft, compared with an average of 13%, and 27% have experienced information theft, compared with an average of 22%.

While this sector seems to suffer less than most from corporate fraud, there is no reason for complacency.

- On average, firms lost U.S.\$4.9m over the past three years from corporate fraud.
- More than eight out of ten firms in this sector have suffered from fraud during that period.
- A higher percentage of companies than usual, 91%, think that their exposure has increased.
- Fewer than six out of ten companies are increasing their investment in IT countermeasures for fraud, and less than half are doing so for IP monitoring.

This sector is doing well but should increase its existing efforts, especially in the areas of information technology and intellectual property.

Written by The Economist Intelligence Unit

Challenging corruption in the energy sector



For energy companies, especially those in the upstream oil and gas sector, combating fraud of all types is an everyday challenge embedded in their operating environment. The sheer scale and complexity of the industry and the vast revenues projects can generate even when energy prices are relatively low, explain the challenge.

Knowledge is power and much of the fraud found in the industry revolves around information-seeking. The capital intensive projects of energy companies cost billions of dollars and take years to plan and complete. With so much at stake and fierce competition among potential suppliers

and contractors, details of bid documents are an especially valuable commodity.

In addition to obtaining details about bids, suppliers and contractors try to outdo their competition in the intelligence-gathering business, which in some cases further leads them to illicit tactics including bribery. A cottage industry of “agents” has arisen to “service” the industry, and their audacity is legendary: “We’re pretty clean otherwise,” said one industry executive, “but when it comes to tenders and information on things like production-sharing contracts or details of a deal that another company has cut, well, that can be a different story.”

Energy companies also have to contend with operating in developing countries that lack transparency and have widespread corruption within their private and public sectors. An industry adage calls it “God’s little joke” that much of the world’s oil and natural gas reserves are found in countries that consistently rank among the most corrupt in international surveys. In spite of rigorous and institutionalized risk management structures in the industry, 22 percent of cases filed in the United States under the Foreign Corrupt Practices Act have involved energy companies.

Structural changes in the industry over the past decade may have added to the vulnerability of international energy companies. The use of contractors and consultants has risen sharply to reduce costs. Direct evidence that this trend has led to greater fraud is scant, but anecdotal evidence suggests that the priorities and loyalties of contractors and sub-contractors may not always align with those of the energy company they work for.

Another factor that increases the potential risk of fraud is what some in the industry term the “tyranny of net present value.” On very large-scale projects time is literally money. The strict schedules imposed by project managers can sometimes influence contractors to “cut corners,” even if such actions violate a company’s code of conduct or the contract terms.

With perhaps half of all major energy infrastructure projects over budget and significantly late, such pressure can be overwhelming. “If part of a project is falling badly behind schedule for non-technical reasons, such as labor unrest or the failure of a ministry or local government to issue the right permits in a timely manner, then

there is always a temptation to facilitate the process,” said one veteran project manager for an international oil service firm. “Sometimes we can solve the problems with community or social investment. Sometimes we can just talk our way through the issue, but sometimes not.” Contractors also know that as a project progresses, the balance of power often shifts in their favor, and that companies may turn a blind eye to transgressions.

Finally, the emergence of “resource nationalism” in recent years, on the back of a global boom in commodity prices, has also transformed the industry’s competitive landscape. Many western companies now chase fewer and fewer opportunities, especially in the developing world. Energy firms from countries such as China have made deep inroads in many places, such as Africa, largely because they are not subject to the rigorous governance guidelines of their western counterparts.

It is unfair and inaccurate to say that the global energy industry has a “corruption culture,” as some critics contend, especially given the significant progress made in recent years on a wide range of transparency, governance, and anti-corruption issues. As many in the industry wryly note, however: “rule number one is that it’s all about the money and rule number two is never forget rule number one.”

Robert Corzine is a specialist in corporate communications, public relations and public affairs. He has particular expertise in the energy and natural resource sectors. He is the former Energy Correspondent of the Financial Times and has provided strategic and communications advice to Royal Dutch Shell and BP among others.

EIU SURVEY

Fraud presents a big challenge to the natural resources industry.

- Companies consider themselves most exposed to corruption with nearly one-quarter ranking their firms as highly vulnerable, which is almost double the average. One in five puts themselves in the same category with respect to information theft.
- The loss per company during the past three years has been U.S.\$11.5m, more than 70% higher than the average.
- The prevalence of corruption, which is reported by 20% of firms in this sector, is very close to the average of 19%, while the prevalence of information theft, which is reported by 15%, is well below the average of 22%.
- Businesses in this industry are more likely than average to face issues of theft of physical assets, which has been experienced by 39%, management conflict of interest, experienced by 31%, or regulatory breaches, experienced by 24%. Perceived vulnerability in these areas, however, is roughly similar to that of the survey average.

The sector’s willingness to address a range of threats limits damage.

- For nine out of the ten anti-fraud strategies listed in the survey, adoption within the sector was noticeably more widespread than the average, usually by about 10%. Financial controls, for example, were used by more firms to combat fraud than any other sector, including financial services.
- A higher than average proportion of natural resource firms was also planning additional investment for seven out of the ten strategies. Protection of physical assets – theft of which represents the most common problem – will see the most widespread attention, with 62% of firms spending here. This is well ahead of the 45% average.

Despite the high cost of fraud per company, these efforts by the sector are having some positive effects.

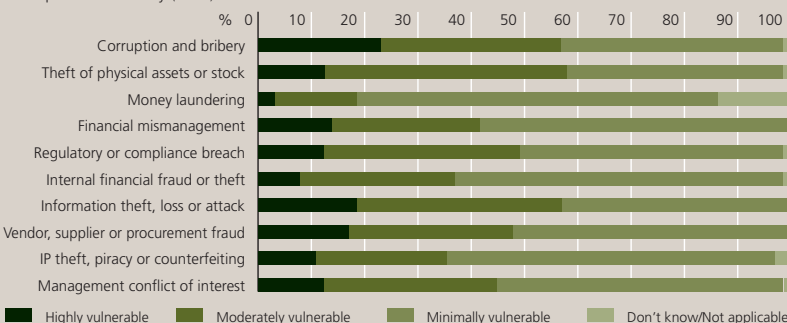
- Thirty-four percent of companies report suffering no fraud at all within the past year, which is well ahead of the overall average of 19%.
- Fraud exposure has stayed constant or declined at 28% of firms, compared with 18% for business as a whole.

The high loss per company, spread over a relatively low proportion of firms actually affected by fraud, indicates that, when something goes wrong in this sector, it is extremely costly. Some firms may need to increase their already above-average efforts, and it is possible that they could benefit from a deeper understanding of the particular threats they face.

Written by The Economist Intelligence Unit

REPORT CARD NATURAL RESOURCES

Financial Loss: Average loss per company over past three years: U.S.\$11.5m (171% of average)
Prevalence: Percentage of companies suffering losses from corporate fraud over past three years: 66%
Increase in Exposure: Percentage of companies where exposure to fraud has increased: 72%
Areas of High Vulnerability Corruption and bribery (23% of sector firms indicate that they are highly vulnerable to this threat) • Information theft, loss or attack (19%)
Areas of Frequent Loss: Theft of physical assets or stock (39% have experienced in past three years)
 Management conflict of interest (31%) • Regulatory or compliance breach (24%)
 Corruption and bribery (20%)





Unique profile of the airline industry

The airline industry is unique in many ways: its scale, its history, and – unfortunately – its exposure to fraud.

The *Airline Fraud Survey 2006*¹ puts the cost of fraud to the airline industry at over \$600 million a year, or an average loss of \$3 million per company. The types of fraud it identifies include counterfeit or stolen tickets, cargo theft, false baggage claims, and frequent flyer abuse. The biggest losses, however, come from credit card fraud. The survey claims that approximately 60% of airlines have no anti-fraud program in place, do not perform frequent fraud risk assessments, and have no process to track or record fraud, while over a third discover fraud “by accident”.

Surveys inevitably do not reflect the full extent of the problem as much fraud will certainly not be “self-confessed” or revealed as a result of a questionnaire. Secondly, the true scope of fraud cannot be quantified. The exposure airlines face is substantial

and only a fraction of it is known or even considered.

The large number of areas exposed makes the fraud profiles of these companies unique. The problems are compounded by large staff requirements, operations in many countries and languages, and dealing with hundreds of suppliers, from the large – aircraft and fuel – to the tiny – peanuts and mini pretzels.

Our work with airlines suggests that the areas vulnerable to material frauds include, but are not limited to, the following:

- Management of airline property
- Ground-handling contracts
- General sales agents contracts
- Third party maintenance and engineering contracts
- In-flight and catering supplies
- Aircraft and engine leasing
- Fuel purchasing

- Cargo operations
- PR and marketing contracts
- Internal finance / treasury / revenue accounting manipulations

The potential for fraud represents a significant risk to an airline and can have critical consequences when margins are tight. It is not easy to combat the problem across extensive areas. Even the most robust internal controls are severely strained under such demands.

The primary responsibility of ensuring total safety and security on each and every flight further complicates the task for airlines.

Airlines should establish their own dedicated fraud departments.

What can be done? We believe that, because of their unique exposure, airlines should establish their own dedicated fraud departments (drawing on Internal Audit and Security) in pursuit of two principal objectives: to put in place an internal control system that is constantly monitoring for signs of fraud, and to increase the effectiveness of the company's anti-fraud culture through training and the use of integrity reporting lines. Success, however, will require the highest levels of support from senior management and an acceptance that it will be a challenge that reaps the benefits of the energy put into it.

¹ Deloitte and the International Association of Airline Internal Auditors



Charles Carr is a managing director and head of Fraud for Europe, Middle East and Africa. He was previously head of the Milan office and country manager for Mexico and specializes in fraud prevention programs and training. He previously spent time as an oil futures broker for Kidder Peabody.

REPORT CARD TRAVEL, LEISURE AND TRANSPORTATION

Financial Loss: Average loss per company over past three years: U.S.\$1.1m (16% of average)

Prevalence: Percentage of companies suffering corporate fraud loss over past three years: 80%

Increase in Exposure: Percentage of companies where exposure to fraud has increased: 70%

Areas of High Vulnerability: Information theft, loss or attack (13% of sector firms indicate that they are highly vulnerable) • Internal financial fraud or theft (13%)

Areas of Frequent Loss: Theft of physical assets or stock (42% have experienced in past three years) Management conflict of interest (30%) • Internal financial fraud or theft (27%) • Corruption and bribery (24%) Vendor, supplier or procurement fraud (21%)



The gambling industry and money laundering

Gaming and gambling are important global industries, and the majority of firms are run legally and soundly. But the gambling industry attracts money launderers, offering a variety of ways for illegal funds to be apparently bet but in fact laundered. One example is the purchase of a large number of casino chips, which are then cashed in as if they were winnings from a “lucky run”. Online betting is also useful for hiding the illegal origin of money. Many casinos are open twenty-four hours a day and anyone can play. Moreover, Internet bets can be made by credit card, increasing the risk of fraud. Many jurisdictions therefore tightly regulate this industry, whether the bets are physical or virtual.

The 9/11 terrorist attack brought in its wake American legislation to impede money laundering and terrorist funding, which has deeply affected the gambling industry. The U.S.A. Patriot Act, for example, included important and far-reaching “extraterritorial” provisions that changed the outlook for companies bound by U.S. law. Companies linked to service providers – in this context examples include those providing slot machines, gaming software, mutual betting system administration, instant lottery

administration, or electronic gambling games – or firms with partners located on U.S. territory, find themselves indirectly bound to comply with the legislation, even when the country in which they are conducting business has little or no regulation in this regard.

Although money laundering cannot be completely avoided, it is timely for gambling companies to develop policies and procedures that improve and extend existing controls against this practice, as well as against more general fraud and terrorist funding. Those working on such policies must consider areas including: identifying, and finding out details of, betters, winners, and employees; and defining operational procedures and different gambling methods according to the risks they represent.



Karla Sotomayor is an associate managing director in Mexico. She has spent over 10 years working in anti-money laundering and compliance and previously worked as anti-money laundering director at Banamex/Citigroup.

She is a member of the Mexican Bar Association.

EIU SURVEY

Overall, the travel and leisure industry suffers comparatively few problems from corporate fraud.

- The loss per firm during the past three years was \$1.1m, or one-sixth of the average, although this is partly due to the lower turnover per firm in this sector, which equates to 80% of the average.
- Overall, fraud has grown slightly less prevalent for this sector during the same period, with just 22% reporting an increase.

Accordingly, companies show only moderate concern about the issue.

- Businesses are less likely to consider themselves highly vulnerable to all types of fraud, with only 13% characterising themselves as such for the most common worries: information theft and internal financial fraud.
- The current use of anti-fraud strategies is very close to the average across the board, leaving 20% making no use of financial controls against these threats, and 30% eschewing IT countermeasures or security systems for physical assets.
- The proportion planning investment in such strategies is also very close to the mean.

Worrying data, however, suggest that more attention is needed.

- Although the costs are still small, the prevalence of certain types of risk are alarmingly high in the travel industry: 42% have suffered from theft of physical assets (the overall average is 34%); 30% from management conflict of interest (compared with 21%); 27% from internal financial fraud or theft (compared with 19%); and 24% from corruption and bribery (compared with 19%). All these tend to balloon if left unchecked, so their wide prevalence, even at low volumes, is a concern.

Although the problem of corporate fraud is not currently as serious as that faced by other sectors, the travel industry must take greater care to ensure that it does not become more prevalent.

Written by The Economist Intelligence Unit

Commodity trading and shipping fraud

The sale of goods across borders poses financial risks for suppliers and purchasers. Many commodities are produced in, warehoused in, or shipped through emerging market countries where corruption and bribery are common. In addition, lengthy trade routes can mean a space of two to three months between the delivery of goods by the manufacturer and their receipt by the end user.

Given this kind of delay, those involved want to protect themselves against financial loss. The supplier, before shipping the goods, wants to be sure of payment and the buyer wants to know, before paying, that the product will arrive. A common way for both parties to protect themselves is for the buyer to obtain a letter of credit from a financial institution that guarantees payment to the supplier once the goods have been received and checked.

As the value of letters of credit increases, so should the level of due diligence performed.

A simple letter of credit works as follows: Buyer A provides collateral to a bank, in exchange for which the bank guarantees to Supplier B that, on receipt of appropriate proof that the goods have arrived at the nominated destination, it will pay to Supplier B the stated amount for them. Supplier B is responsible for providing to the bank the appropriate documentation, and the bank is responsible for checking

that the supplier fulfills the terms of the letter of credit before making payment.

More and more, however, this form of guarantee is providing the opportunity for criminal gangs to conduct fraudulent transactions. Three typical scenarios are:

1. A fraudulent supplier enters into a transaction to provide goods. He obtains a valid letter of credit from a genuine buyer, but provides false documents to the bank, sometimes assisted by corrupt port officials who provide fake bills of lading. The bank pays out on the letter of credit but the goods never arrive.
2. A fraudulent buyer provides a fake letter of credit. The genuine supplier ships the goods. However, when the supplier attempts to draw down on the letter of credit, the bank refuses to pay because it is false.
3. A variant of the above is when a buyer provides a genuine letter of credit for several transactions, usually involving small amounts for which he is able to provide collateral. The buyer then places an order for a much larger quantity and uses a fake letter of credit naming the same bank as the earlier, legitimate ones. The fraudulent buyer then disappears when the large order has been delivered (and sold for a profit).

In all of the above scenarios, it is very difficult for the genuine party to insure that it has fully protected itself against fraud. In the first case, where corrupt port or warehouse officials are providing genuine confirmations, the only way for the buyer to verify these documents is to have



someone physically check in the port that the goods exist. Kroll's international presence and extensive network of investigators in the major port cities mean that clients instruct us to verify the existence of goods being stored or shipped.

In the second example, especially as Western businesses increasingly deal with emerging-market banks, it is difficult for companies to know the authenticity or the creditworthiness, of the banks providing the letters of credit. Once again, Kroll is instructed to conduct due diligence both into the financial institutions issuing the letters of credit and into the authenticity of the letters themselves.

In the final scenario, companies should be careful about new customers who quickly build up large credit positions. They should continue to conduct the necessary due diligence and insure that their standard credit procedures are followed, no matter how good a prospect a new customer might seem. As the value of the letters of credit increases, so should the level of due diligence performed on the customer, the issuing bank and the letter of credit.

The international commodity trade presents great opportunities for both honest and dishonest operators. Awareness of the latter's techniques can help the former avoid fraud.



Richard Abbey is a managing director and head of financial investigations in London. He specializes in managing complex and multi-jurisdiction frauds and asset tracing including the collapse of Parmalat Spa and Barings Bank. Prior to this he worked at Ernst & Young. He is a chartered accountant and Certified Fraud Examiner (CFE).

REPORT CARD RETAIL, WHOLESALE AND DISTRIBUTION

Financial Loss: Average loss per company over past three years: U.S.\$1.9m (29% of average)

Prevalence: Percentage of companies suffering corporate fraud loss over past three years: 84%

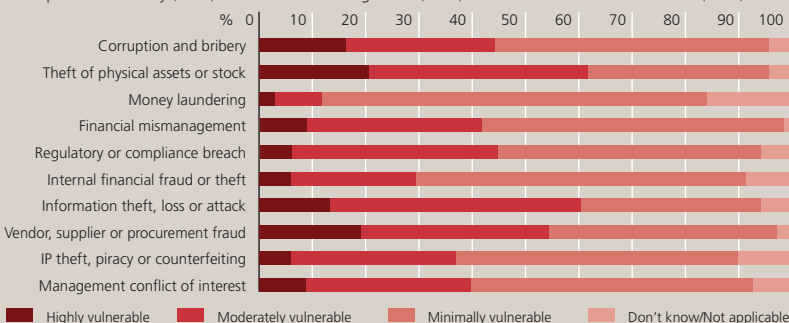
Increase in Exposure: Percentage of companies where exposure to fraud has increased: 76%

Areas of High Vulnerability: Theft of physical assets or stock (21% of sector firms indicate that they are highly vulnerable) • Vendor, supplier or procurement fraud (19%)

Areas of Frequent Loss: Theft of physical assets or stock (44% have experienced in past three years)

Vendor, supplier or procurement fraud (31%) • Information theft, loss or attack (29%)

Corruption and bribery (25%) • Financial mismanagement (24%) • Internal financial fraud or theft (22%)



Working out weak points can pay off

“Why didn’t internal audit catch this?”

This is a common refrain among senior executives every time a weakness in a company’s controls or a new fraud is discovered, despite all the new technologies, controls, regulations, and money spent to catch thieves. The answer is usually something like: “nobody knew we were vulnerable;” “these guys were clever;” or “it’s not something that we audit, and we didn’t identify it in our risk assessment.” While you may want to reply “why not?,” the real response could be, “we need to think like a fraudster and conduct a fraud vulnerability assessment.”

Fraudsters are not necessarily clever. More often they are merely motivated, willing, and able to take advantage of vulnerabilities in the process or controls. How do they discover these? By mistake; sometimes by testing systems out of curiosity; most times because of their intimate knowledge of the systems or processes. Often a loophole is developed as a workaround by an employee looking for a better way to do his or her job. Unfortunately, these workarounds usually circumvent internal controls.

Think like a fraudster and conduct a fraud vulnerability assessment.

What happens when internal controls are avoided?

A third party logistics and fulfillment company prided itself on its ability to control its customers’ high-end electronics inventory. The company had instituted a robust “cycle count” program that allowed it to communicate with every stock keeping unit at least once every 30 days. This allowed the company to eliminate the need for a wall-to-wall physical inventory, provided timely visibility to shrinkage issues, and allowed for detailed reporting to clients. The system worked unless an item could be intentionally left out of the “cycle counts.”

An investigation determined that items to be counted were based, in part, on the last count date – a field that could be manipulated in the Excel spreadsheet running the program. Because the dates could be manipulated, the inventory counters could avoid counting any specific

item. This workaround demonstrated that high-value goods could be stolen surreptitiously in the same manner. Before inventory levels had declined significantly for the fraud to be discovered, the bad guys had moved hundreds of thousands of dollars of material from the facility.

Smarter thieves would not have allowed these levels to get low, and their scheme would have lasted much longer. Fortunately, most fraudsters do not thoroughly think through the ramifications of their actions. In any business with inventory, this type of theft can directly affect the bottom line and, perhaps more importantly, damage a relationship with a customer.

The problem was discovered because a fraud investigator simply asked if it could be done. How did he know to ask? Experience. It is one of the hundreds of hidden vulnerabilities examined in a proactive fraud vulnerability assessment.

Prevention or detection?

In Kroll’s experience, companies conduct many investigations after a theft is discovered, but often are unwilling to conduct a fraud vulnerability assessment which could prevent it from occurring. The most common explanations are that margins are tight, resources thin, and the immediate payback neither quantifiable nor material. However, many frauds could go undetected precisely because they may not have a material impact on the financial statement. Additionally, if a company is publicly traded, it may consider its efforts to comply with Section 404 of the Sarbanes-Oxley Act (where issuers are required to publish information in their annual reports concerning the scope and adequacy of the internal control structure and procedures for financial reporting) sufficient.

The reality is that an immediate payback often occurs. In most cases, fraud vulnerability assessments identify fraud, waste and abuse well in excess of the cost of the review. Teaming up experienced fraud investigators with internal auditors, physical security, and information technology specialists to conduct these reviews and examine every department helps set the proverbial “tone at the top.” Most important, the investigative team identifies the workarounds and loopholes before the bad guys begin exploiting them. This protects a company’s financial statement, reputation and customer relationships.



Mark Sullivan is a managing director in Chicago specializing in fraud detection and prevention. He was previously Deloitte & Touche’s practice leader of corporate loss prevention and is a visiting lecturer at the University of Wisconsin’s

Forensic Accounting program. He is a Certified Fraud Examiner (CFE).

EIU SURVEY

Unsurprisingly, companies in this sector face a particular challenge from types of fraud involving physical goods. Other types of corporate fraud also pose problems, but they tend to be less severe than for businesses in most other sectors.

- More than one in five retail, wholesale and distribution businesses consider themselves to be highly vulnerable to theft of physical assets, and an alarming 44% have experienced this problem in the past three years.
- Procurement fraud is a similar worry for almost as many companies (19%) and 31% of companies have experienced this problem in the same time period.
- Information theft, corruption and financial mismanagement have all been experienced by roughly one-quarter of businesses.
- Three-quarters of firms in this sector believe that their exposure to fraud has increased, although this is slightly lower than the average for all industries of 81%.
- Respondents from this sector indicate that fraud has grown slightly less prevalent, and that the loss from it per company was only \$2.9m over the past three years, which is less than one-third of the average.

A lack of focus on pressing issues may hurt the sector’s relatively positive performance.

- Although information theft is one of the most widespread types of fraud for these firms, affecting 29%, only 57% currently deploy IT countermeasures, and a similar number (52%) is looking to invest in this area in the future. These are both figures that are well below the overall averages (70% and 59%).
- Weaker internal controls have increased exposure at 31% of companies.

Companies in the sector will need to maintain or increase their vigilance in order to keep up their relatively strong performance against corporate fraud and to reduce the worrying frequency of several particular types of it.

Written by The Economist Intelligence Unit



Brand integrity: Anti-counterfeiting, piracy and tainted goods

Antifreeze-tainted toothpaste, lead-painted toys, tread-splitting tires, contaminated pet food, dangerous pharmaceuticals, pirated software – for the past several months, one counterfeit product or tainted ingredient entering the Western marketplace after another has been in the news. Almost without exception, these products originate partly or solely in China.

This coverage has captured the attention of consumers, regulators, and corporations alike. Beyond returning their suspect toys and checking their toothpaste, individual consumers cannot do much. No matter how vigilant they may be, it is virtually impossible for an individual to be completely sure that a particular product is safe for their family. To minimize their exposure, most rely on trusted brands made by trusted manufacturers. Implicitly, consumers also put faith in the global regulatory agencies that monitor product manufacturing and distribution.

Regulatory and enforcement agencies are doing what they can: recently in the United States, the Federal Bureau of Investigations

seized \$500 million worth of pirated software; Congress held hearings on food safety; and the Food and Drug Administration signed an agreement with the European Food Safety Authority to improve the assessment of food safety risks.

Global consumer product manufacturers must serve as their own regulators and enforcers.

In China, the execution of Zheng Xiaoyu, a corrupt State Food and Drug Administration official, clearly indicated that the government recognizes the seriousness of the situation. Beijing officials have announced wide-ranging measures to curb counterfeiting, including the hiring of an American crisis manager to improve a tarnished image and secure the future of lucrative trade relationships with Western countries. A quote from a Chinese government official in a recent CNN.com

article, however, pinpointed the underlying problem: “As a developing country, China’s food and drug supervision work began late and its foundations are weak.”¹¹

For far different reasons, the United States also finds itself in a dismal situation, with regulatory agencies ill-equipped to deal with counterfeiting or to assure the safety of imports. In Western countries, the issue is not lack of a foundation for supervision, but the reality of globalization and the vast growth in the number of products that arrive from abroad. To compound the problem, counterfeiters are growing ever more sophisticated, often becoming involved in organized criminal networks and leveraging technology and the Internet to avoid detection.

This combination of globalization, advanced technology and an under-resourced regulatory and enforcement environment creates a world of opportunity for counterfeiters. Unfortunately, the increasing number of news reports referred to earlier heralds a problem that is increasing in scale.

Global consumer products manufacturers cannot rely on government alone, but must serve as their own regulators and enforcers to assure the well-being of their consumers and the security of their brands. New York Senator Charles Schumer warns business: "You better protect yourself because right now neither the Chinese government nor the American government is doing a very good job of protecting you."²

The responsibility for protecting their brands in the marketplace goes hand in hand with the privileges and protections that manufacturers gain from intellectual property and trademark regulations. Corporate social responsibility for consumer-facing multinationals must include a dedicated effort to protect those who use their products. While business leaders clearly face other great pressures, doing nothing in response to this problem poses unquantifiable tangible and intangible risks. In Kroll's experience, inaction almost always costs more to business than focused investment in brand protection and crisis prevention programs that can arise from counterfeit or tainted products. While there is no "cookie cutter" formula for such a strategy, the most effective approaches typically share the following common elements:

- **Detection:** Immediate, aggressive and relentless investigation of reports of counterfeit or tainted products is essential;
- **Aggressive Enforcement and Deterrence:** A commitment to punishing infringers with more than a slap on the wrist is key;
- **Prevention:** Build in protection at the development stage and implement IP security in operations. Vet suppliers,

manufacturers and distributors who are involved in the manufacturing process;

- **Supply Chain Management:** Companies must know who is touching their product and all of its component parts at every step along the chain and keep an eye on these operations throughout the process;
- **Monitoring:** Companies must be vigilant that no dangerous versions of their product reach retail shelves or the hands of consumers.

Governments can never replace the role of private companies in protecting their own brands and the customers who consume them. A well thought-out strategy can go a long way toward fulfilling that responsibility.

¹ <http://www.cnn.com/2007/WORLD/asiapcf/07/10/china.execution.reut/index.html>

² New York Times, 1 July 2007

Steven Rucker is an executive managing director based in New York. He specializes in litigation support, product tampering and patent infringement. He previously worked as deputy commissioner for the New York City Department of Investigation, where he managed cases involving corruption.

Richard Plansky is a managing director based in New York. He specializes in the protection of intellectual property and the loss of proprietary data. He previously worked as deputy criminal justice coordinator for the Office of the Mayor of the City of New York and served as assistant district attorney for New York County.

Adrienne Gaboury is an associate managing director based in San Francisco. She has conducted cases on intellectual property infringement, business controls reviews and brand monitoring. She is a member of the Association of Certified Fraud Examiners (ACFE).

EIU SURVEY

The consumer goods sector is the least troubled by corporate fraud among the industries questioned for our survey.

- The loss per company is approximately U.S.\$600,000, or just 9% of the average, despite the typical respondent in this sector having a higher turnover than most.
- Perceived risk is very low compared with other sectors. IP theft is the type of fraud to which the greatest number of respondents in this sector consider themselves to be highly vulnerable, but only 11% claim that they fall into this category.
- Thirty-two percent of firms have suffered no corporate fraud in the past three years, which is more than 50% better than the survey average. The prevalence of every specific type of fraud is also lower in this sector, often significantly so, except for theft of physical property and IP theft, both of which are close to the average for the overall sample.
- Thirty-four percent of firms have seen the prevalence of fraud decrease and only 23% experienced an increase.

However, a very good relative position does not mean that fraud has ceased to be a problem.

- During the past three years, more than two-thirds of firms have suffered from corporate fraud in this sector.
- Seven in 10 have seen their exposure increase.

One reason for the sector's success in containing fraud has been how seriously it treats the problem.

- Use of the most important anti-fraud strategies is more widespread in the consumer goods sector than elsewhere. Financial measures are used by 83% of these firms, against 79% for the average. The spread in other areas is more pronounced, information security is used by 83%, compared with 70% for the average; physical asset security is used by 79% compared with 67%, and management controls used by 69%, compared with 64%.
- Planned investment in further security measures is also more widespread across the board than in other sectors. For example, 69% plan further investments in information security, against an average of 59%.

The consumer goods sector is working hard to combat corporate fraud, and the results show. Although well ahead of its peers, plenty of scope remains for further progress.

Written by The Economist Intelligence Unit

REPORT CARD

CONSUMER GOODS

Financial Loss: Average loss per company over past three years: U.S.\$0.6m (10% of average)

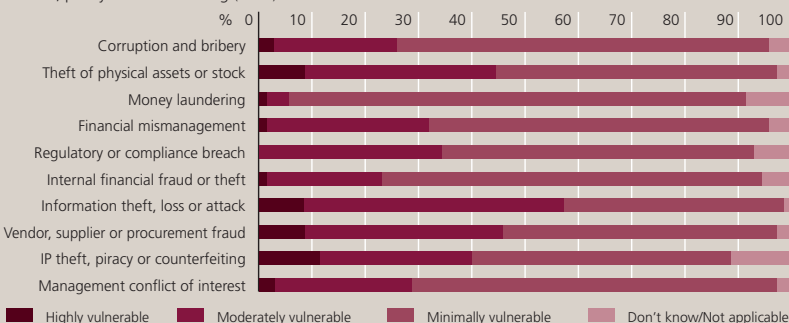
Prevalence: Percentage of companies suffering corporate fraud loss over past three years: 68%

Increase in Exposure: Percentage of companies where exposure to fraud has increased: 70%

Areas of High Vulnerability: IP theft, piracy or counterfeiting (11% of sector firms indicate that they are highly vulnerable) • Information theft, loss or attack (9%)

Areas of Frequent Loss: Theft of physical assets or stock (39% have experienced in past three years)

IP theft, piracy or counterfeiting (20%)



Audits, screening, and expertise help to build integrity

Construction fraud can happen on any kind of project: large or small, public or private, commercial or residential, new building or renovation, small town or big city, American or international. Having investigated hundreds all over the world, I have not come across one that was totally clean. Just Google the words “construction” and “fraud,” and you get a staggering, almost endless list of projects that have been the subject of fraud and corruption.

In Britain, for instance, the Office of Fair Trading this year uncovered the largest bid-rigging cartel in its history: nearly 100 companies, some among the country’s largest, fixed thousands of contracts valued in excess of \$6 billion. In China, the Ministry of Railways is investigating the widespread use of fake materials in the \$12 billion construction of hundreds of kilometers of high-speed passenger railway. In Brazil, federal police in May arrested 47 people tied to a complex bid-rigging and kickback scheme on public works projects worth millions of dollars. Twelve legislators have been implicated.

Transparency International, the anti-corruption NGO, estimates that 10% of total worldwide expenditure on construction is lost to fraud and corruption. In 2001, Britain’s National Audit office estimated that the same amount is lost this way in the United Kingdom. In the United States, every month a press release from the Department of

Justice or a state, city, or county agency announces arrests, indictments, or convictions that support this 10% figure.

So what do you do if you are facing a construction project that you know has a significant risk of fraud and corruption but want to protect your corporate reputation and pocketbook? Regardless of where your project is, or your role in it, consider the following:

- Do not rely on construction experts to police fraud risks. General contractors (GCs), construction managers (CMs), subcontractors (also called vendors), project consultants, architects, designers, engineers, or even your own internal facilities people are not fraud prevention and detection specialists. The pervasive fraud in the industry shows that using them in this way will not work.
- Gauge the fraud risks in the project’s procedures. A fraud vulnerability assessment on contracts, procurement, and requisition, as well as on materials and equipment receipt, usage, and storage processes greatly enhances your team’s capabilities and will act as a significant fraud detection and prevention mechanism.
- Institute a vendor screening process. This will greatly reduce the risk of vendor-related fraud and give you critical information about a vendor’s business history, reputation, safety record, and

financial health. Also, institute a vendor Code of Ethics. Effective screening will eliminate organized crime-controlled subcontractors, as well as identify improper conflicts of interest, fictitious vendors, and false or misleading documentation. Do not rely on GC/CM representations about the vendor for fraud prevention.

- Have a fraud expert oversee aspects of procurement. Independent oversight of the bidding process will ensure a level playing field, the confidentiality of important bid information, identify or deter bid-rigging, and insure that estimates and proposals do not contain fraud.
- Have a fraud specialist conduct random and periodic forensic audits of requisitions and supporting documentation. With proper audit rights on GCs/CMs and vendors, the review will greatly reduce a whole host of manipulative and abusive practices. Do not rely on project auditors to conduct this review: their role is to reconcile costs, not forensically analyze them.
- Conduct random on-site audits. Have a fraud expert discreetly track site labor, materials usage and storage, equipment usage, and safety and security issues. This will substantially decrease the use of unskilled, non-union, or non-existent labor; no-show or no-work jobs; inferior, over-purchased, or substituted materials; theft of site property; on-site gambling, drug dealing, and alcohol abuse; and the presence of organized crime and union corruption by insuring compliance with collective bargaining agreements. It will also help the forensic review.
- Understand that the nature of your contract does not protect you against cost abuses. Fraud and corruption is an equal opportunity abuser. A fixed-price contract may protect you against cost overruns, but it will not protect you against abuses within the initial scope costs or stop organized criminal activities, union corruption, labor or material misuse schemes, or false billings.

The above safeguards need not adversely impact project costs or scheduling. They will act as both a significant deterrent to fraud and a detection measure that could save you at least 10% to 12% of your project’s costs, safeguard your image and reputation, and minimize your future liability, all while costing a fraction of the amount saved.



Blake Coppotelli is a senior managing director 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.

REPORT CARD CONSTRUCTION

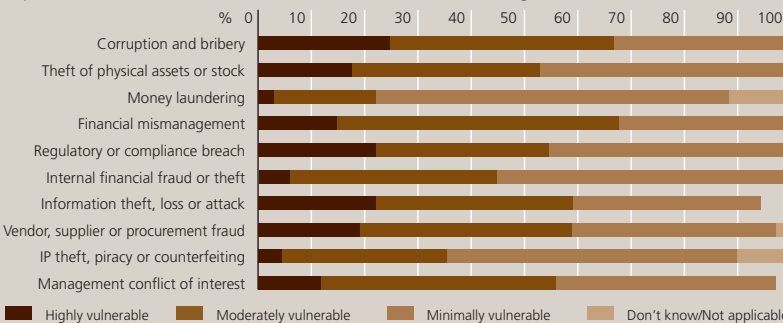
Financial Loss: Average loss per company over past three years: U.S.\$4.5m (67% of average)

Prevalence: Percentage of companies suffering corporate fraud loss over past three years: 77%

Increase in Exposure: Percentage of companies where exposure to fraud has increased: 87%

Areas of High Vulnerability: Corruption and bribery (25% of sector firms indicate that they are highly vulnerable to this threat) • Regulatory or compliance breach (22%) • Information theft, loss or attack (22%)

Areas of Frequent Loss: Theft of physical assets or stock (44% have experienced in past three years) • Corruption and bribery (33%) • Financial mismanagement (30%) • Regulatory or compliance breach (25%) • Vendor, supplier or procurement fraud (23%) • Internal financial fraud or theft (22%) • Management conflict of interest (22%)



Transparency is the key to monitoring the supply chain

Large scale projects, such as those in the construction industry, commonly involve multiple suppliers and subcontractors. The costs and complexity associated with these contracts can make them a target for fraud. Even companies with excellent internal controls can still find themselves exposed when their requirements for probity are not followed further down their supply chains. Kickbacks, collusion between contracted suppliers, price rigging, and over-specification are just some of the means by which suppliers can expose companies to such risks. Supplier fraud can increase costs, lengthen timescales, and jeopardize a project's very viability.

Existing measures, such as supplier accreditation and employee checks, are essential to protect against companies and staff who might engage in malpractice. But these alone are insufficient to protect a business against supplier fraud, particularly in high-cost projects. To protect themselves properly, companies must be prepared to exert their influence further along the supply chain, so that the levels of probity and compliance required do not just stop at its front door.

How can firms better protect themselves against supply chain fraud?

1. Audit the processes suppliers have used to select subcontractors.

This should include auditors and procurement managers seeing details of whether the supplier tested the market when selecting the subcontractor, and the outcome of this process.

2. Monitor any contracts to be subcontracted by suppliers during a project.

If contracts are to be subcontracted, the contracting organization should demand visibility of the associated procedures, specification, and documentation. Audit managers need to be confident that contracts are being subcontracted with robust processes, and that best value is

being achieved through the supply chain. If necessary, tenders can be brought into the original contractor's procurement department to insure compliance.

3. Extend internal anti-fraud procedures to suppliers.

Large scale capital projects are likely to require significant interaction between companies and their suppliers. Supplier staff members are no more or less likely to encounter or commit fraud. Companies therefore benefit from extending any anti-fraud measures, such as whistle-blowing lines and employee checks, down the supply chain to their suppliers and subcontractors.

4. Adopt open-book accounting.

With open book accounting for projects, suppliers provide details of all their costs on a project and work to an agreed set of mark ups and margins. This practice enables a company to monitor its supply chain, and prevent price rigging or invoice inflation.

5. Run a good procurement function.

A good understanding of a market's dynamic is the best tool for protecting against price rigging and over-specification. Procurement professionals with an expertise in particular markets can provide companies with sound pricing knowledge, market intelligence on supplier performance, and negotiation skills.

The likely costs and resources required to defend against procurement fraud committed by suppliers are considerable but, in capital projects that cost millions, these need to be weighed against the potential impact of fraud. The costs of project delays, project failures, investigations, and the legal fees required to seek redress will far outweigh those of working with suppliers to protect a company's interests during a project.

Ian Makgill is the founder and head of consulting for Ticon UK. He has co-authored the chapter on e-procurement for the National Procurement Strategy.



EIU SURVEY

In many countries, this industry has a reputation for problems with corporate fraud, and the survey findings bear out the perception that it represents a significant challenge.

- Construction firms are unusually exposed to a broad range of risks: one-quarter consider themselves highly vulnerable to corruption and bribery, and about one in five feel the same way about compliance breaches, information theft and procurement fraud. All these figures are higher than the survey averages.
- In general, the construction business suffers from a much higher incidence of corporate fraud than other industries. Particular problems include the theft of physical assets (44% of sector firms have experienced this compared with 35% on average), corruption and bribery (33% compared with an average of 19%), financial mismanagement (30% compared with 20%) and regulatory and compliance breaches (25% compared with 19%).
- Construction even has the second highest prevalence of money laundering after the financial services industry (albeit still a low figure). It is a problem that affects 7% of firms.
- Respondents indicate that this high level of corporate fraud has, if anything, increased slightly over the past three years, with 32% seeing an increase and 29% a drop.
- Construction is experiencing a greater exposure to fraud through high staff turnover (46%), entry into new markets (44%), and increased collaboration (35%) than is experienced by other industries.
- Thirty percent face increased exposure after having weakened existing internal controls.

Despite these very widespread problems, the response to corporate fraud has been muted so far. Small signs of change are, however, appearing.

- The proportion of construction companies using anti-fraud strategies, such as financial controls, physical security systems and management controls is slightly higher than in other industries, but the sector lags behind in IT security.
- A higher proportion of construction firms than the average are investing further in these strategies.

The construction sector has a long way to go, but seems to be making a tentative start. It needs to increase its efforts.

Written by The Economist Intelligence Unit

Red flags:

Behavior that may reveal problems

Knowing why and how fraud infiltrates a project is the first step in stopping it. This article lists some red flags.

Civil construction projects involve a wide-ranging and complex division of work. Each stage has different managers in charge from the previous one, with the project manager left to provide coherence across all the activities. Moreover, each project gives rise to diverse documents, contracts and other legal papers. This all creates huge difficulties for builders and their clients trying to assure the quality of the work, avoid financial waste and protect against dishonest companies.

Based on our experience, Kroll believes that the most common areas of fraud in this sector involve:

- Receipt of kickbacks from suppliers;
- Misappropriation of materials;
- Embezzlement of funds;
- Over-billing in contracts, often to cover up kickbacks or even theft;
- Non-compliance with measurement, material quantity and quality specifications;
- Bribes to procure inside information during the bidding process;
- Bribes to insure tender notices bear specifications that only a particular company can meet;
- Bribes to secure environmental licenses.

The largest frauds are generally committed by people who have performed the same job for a very long time, who act independently of the usual checks and approvals and who hold vast knowledge of the sector's processes and loopholes.

Companies are most at risk when hiring service providers and purchasing materials without taking the proper precautions.

Sometimes businesses operate in distant, remote places, far from cities and business centers, where there is little choice of service providers. In that situation, builders should screen providers carefully. When a great variety of service providers exist, it is important to hold a bidding process with clear estimates, and preferably at least three participants. Always be suspicious when it is impossible to get exact values for the costs of goods, material or services, or when the bid does not explain exactly what will be done and how. Items such as labor costs, land-moving costs, machinery transport, extra or complementary services, and all items preceded by the words "various," "other," or "miscellaneous" should raise red flags. When specific expertise is needed, such as in tunnel drilling or marine excavation, contractors should be selected not only on price, but also on their technical capability and a track record of earlier success.

Contractors should not only be selected on price but also on technical capability and track record.

As for material purchases, employee behavior can be very revealing. Be aware if any of these situations occur:

- If employees always insist on choosing the same supplier without any plausible explanation, even if the price or quality could be better;
- The estimates provided are not presented in a clear, detailed, and standardized way;
- The schedule in the contract is not being complied with;
- Or, the supplier's employees display more wealth than is consistent with their likely wages.



Felipe Soares is a senior analyst in São Paulo. He has been involved in numerous competitive intelligence and asset searches across Brazil.

Where business is feeling the heat

	Corruption and bribery	Theft of physical assets or stock	Money laundering	Financial mismanagement	Regulatory compliance breach	Internal financial fraud or theft	Information theft, loss or attack	Vendor, supplier or procurement fraud	IP theft, piracy or counterfeiting	Management conflict of interest
Construction, engineering and infrastructure	High	High	Low	High	High	Low	High	Medium	Low	Low
Consumer goods	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low
Financial services	Medium	Low	High	Medium	High	Medium	High	Low	Medium	High
Healthcare, pharmaceuticals and biotechnology	High	Medium	Low	Low	High	Low	High	High	High	Medium
Manufacturing	High	Medium	Low	Low	Low	Low	High	Medium	Low	High
Natural resources	High	Medium	Low	Medium	Low	Low	Low	High	Low	Low
Professional services	Medium	Low	Low	Low	Low	Low	High	Low	High	High
Retail, wholesale and distribution	High	High	Low	Low	Low	Low	Medium	Low	Low	Low
Technology, media and telecoms	Low	Low	Low	Low	Low	Low	High	Medium	High	Low
Travel, leisure and transportation	Low	Medium	Low	Low	Low	Low	Low	Low	Low	Medium

Based on data from The EIU Survey

This heat map shows which sectors feel themselves to be vulnerable to particular fraud threats. The point it makes is simple: not every industry (or even company within an industry) will face the same issues: Fraud hits people in different ways at different times, which is why we adapt our solutions to different situations.

- Healthcare, pharmaceuticals and biotechnology is the most vulnerable of the sectors of those we have examined. It sees itself as being at high risk of corruption and bribery; regulatory or compliance breaches; information theft or loss; IP theft; and vendor or supplier fraud.
- The construction, engineering and infrastructure sectors also face serious issues: corruption, theft of physical assets, financial mismanagement, regulatory breach, and information theft or loss.
- Financial services is the only industry that is perceived to face a high risk from money laundering. But it also faces high risks from regulatory and compliance breaches, information theft and conflict of interest.
- Consumer goods considers itself to have a very low vulnerability to fraud overall. However, as our consultants discuss, certain areas – luxury goods, in particular – are vulnerable to IP theft.
- The Natural Resources sector regards itself as highly exposed to corruption and vendor fraud.

- Professional services firms focus on information theft or loss, IP theft and management conflict of interest.
- Manufacturing respondents identified corruption, information theft and conflict of interest as high risks.
- Technology, media and telecoms firms saw information theft and IP theft as significant issues.
- Travel, leisure and transportation regards itself as having a relatively low vulnerability to fraud.
- Retail, wholesale and distribution regards itself as at high risk from corruption, theft of assets and stock, and vendor fraud.

These perceived vulnerabilities did not correlate very closely with the frauds that companies had actually suffered. It seems probable that this is because for a threat to be seen as serious, it is not enough for it to be common. It must strike at a high-value asset, and that asset must be in some way critical to the business. Vulnerability is a function of the likelihood of a threat, but also of its severity.

For example, most had suffered theft of assets or stock, yet few regarded this as a serious threat. There are two likely reasons for this. Firstly, only in some sectors are physical assets so expensive (construction, for example) or theft so widespread (retail) that it is considered a systematic, high-value threat. For the same reason, issues affecting information (information theft or

compromises of IP), and those affecting reputation (corruption, or breaches of compliance and regulations) are taken particularly seriously.

Some threats are seen as “industry problems”: only financial services regards money laundering as a serious risk

No sector regarded internal financial fraud as a high risk, even though it is one of the most commonly reported issues.

We carried out a similar analysis of industry approaches to countermeasures. Unsurprisingly, financial services emerged as the industry that tended to top the list of countermeasures adopted: screening, IT security, reputation monitoring and adoption of risk officers. Natural resources, which has suffered some high-profile issues, was almost as consistent in topping the list of adoption of risk countermeasures: whistleblower schemes, due diligence, media and reputational monitoring, and risk officers.

Overall, the heat map and the analysis of fraud issues supports what any experienced fraud practitioner would suggest: though there are broad trends, each company has its own vulnerabilities to guard against, and its own assets to protect. Generalizing about the scale of fraud, or its incidence, is hard when one is comparing phenomena as disparate as penetration of an information system to steal customers’ details, against the theft of a forklift truck.

Written by **Andrew Marshall**.

The investment herd stampedes into Lagos: Dangers of fraud in a booming market



The flow of capital to emerging markets has boosted demand for Nigerian stocks, bonds and global depositary receipts. New issues, especially in bank shares, are heavily oversubscribed as offshore funds boost the Lagos Stock Exchange to levels which are causing concern locally, if not yet in foreign capitals.

The buying spree by international private equity and hedge funds follows strong gains on the local stock market. Such gains are more the result of government-led restructuring in the banking, insurance, and pensions systems than earnings growth. Nigeria's recapitalized banks have offered a flood of new issues just in time to match demand from global funds.

A period of relatively stable government, steady foreign exchange rates, and moderate GDP growth, underpinned by high oil prices, has restored investor confidence in the Nigerian economy. Nigeria has secured its first-ever investment-grade credit rating and also negotiated the cancellation of most of its foreign debt. This wave of optimism may have obscured the dangers of which investors in this difficult market have long been aware.

By July, the Lagos stock market had risen 50% this year, trading at an average price-earnings ratio of 43, nearly three times that of the Johannesburg Stock Exchange, Africa's only mature and low-risk market. While share prices have risen, dividends

are dropping, and a correction looks almost certain unless companies can find new ways to prop up earnings.

The fraud discovered by Cadbury Schweppes last year at its Nigerian subsidiary was a sharp reminder of the risks of overstated earnings. The confectionery group said that it had discovered "a significant and deliberate overstatement" of Cadbury Nigeria's results after increasing its stake in the business to 50.02% in February 2006. Early this year, Cadbury said that the problems in the country had reduced its 2006 group earnings by up to £53 million, and that Cadbury Nigeria faces lawsuits from local shareholders.

Cadbury has been one of Nigeria's top manufacturers for decades. Its local affiliate had a good reputation for corporate governance and the affiliate's former chief executive, dismissed last year, had recently been named by PricewaterhouseCoopers as Nigeria's "most respected CEO."

The problem at Cadbury Nigeria may be the tip of the iceberg. The fraud was detected after the group changed its local auditors. The previous firm, which had failed to uncover the fraud, audits nearly half the companies listed on the Lagos Stock Exchange.

Local business analysts warn that, although institutions, regulators, and a legal framework are in place, low standards of enforcement and corporate governance place shareholders' interests at risk. Supervision by the central bank and ministerial departments is weak. The

The fraud was detected after the group changed its local auditors.

judicial system is slow and inefficient. Conflicts of interest are routinely flouted. For example, senior market regulators can own their own brokerage firms.

Nigeria's most effective law enforcement agency in recent years, the Economic and Financial Crimes Commission, has a financial intelligence unit to monitor the corporate sector. However, the unit has focused most of its energy on an anti-corruption drive in the public sector.

"If there is ever a major corporate scandal in Nigeria, a local equivalent of a Barings or Enron, capital is likely to be very shy of Nigeria," says Soji Apampa, an academic and consultant who heads the Convention on Business Integrity in Abuja.

Investors would do well to remember that risks do not disappear because everyone else is ignoring them, and that fraud and market bubbles frequently go hand in hand.



Paul Adams is a director based in London. He is a specialist in due diligence and political risk investigations in Sub-Saharan Africa. He previously worked as a journalist for 15 years, including postings at the *Financial Times*, *Reuters*, *BBC World*

Service and *The Economist* in countries including Nigeria, South Africa and Singapore.

The impact of United States regulation on other countries

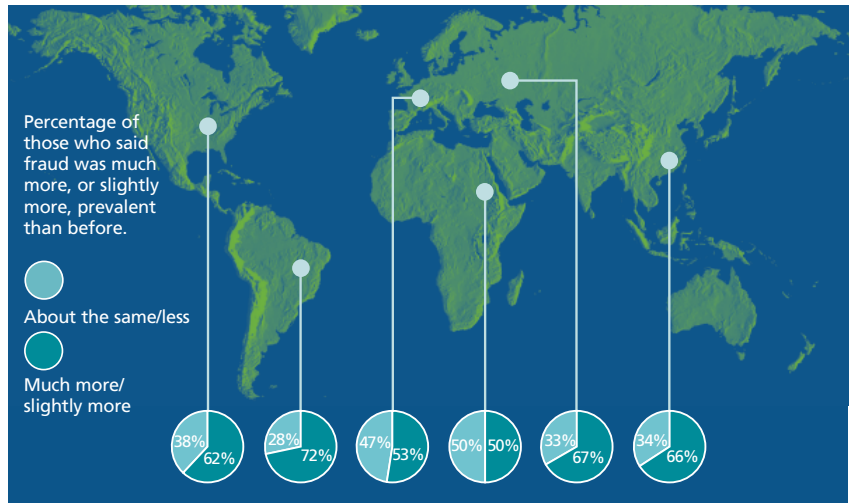
“What happens in Vegas stays in Vegas,” runs the advertising tag line. The implication is that misbehavior doesn’t have to follow you around. As many companies know to their cost, that is no longer true. In particular, it is no longer easy to regard emerging markets as somehow “separate” or different in terms of ethical, reputational or legal behavior.

The U.S.A. Patriot Act, the Sarbanes-Oxley Act, and the Foreign Corrupt Practices Act are just three United States laws that, in seeking greater accountability, transparency, and protection for investors, creditors, and also the public, have changed the international context in which business operates. Actions previously justified as necessary evils to compete in South American countries are now clearly defined by law as acts of corruption and contrary to best practice in good corporate governance.

After 9/11, Congress passed the Patriot Act seeking to end the funding of terrorist organizations. This had a huge impact on domestic financial institutions and companies and also on any businesses that had an interest in maintaining relations with United States entities. Some companies in Colombia found that they needed to improve their money laundering prevention programs and refused to engage in relations with high-risk clients. As a result of the law, the U.S. Department of Justice imposed penalties on United States companies for making payments to guerrilla forces in Colombia. The inclusion of Colombian firms and citizens on the U.S. Treasury’s Office of Foreign Asset Control List means that these companies are now obliged to conduct due diligence investigations into the people with whom they intend to do business.

As the corporate world was adapting to these changes, Sarbanes-Oxley emerged, demanding greater accountability and transparency in order to protect shareholders, investors, employees, and the public against business fraud. Targeted in principle at domestic companies, the law also applies to any firm in the world with a trading or business interest in the United States.

Meanwhile, the Foreign Corrupt Practices Act has re-emerged as a tool for United States judicial and regulatory authorities to



There are some clear regional patterns in terms of the prevalence of fraud as reported by respondents in the EIU survey. Fraud is, broadly speaking, perceived as a greater threat in emerging markets than in developed economies. Some fraud threats have greater regional prevalence, though most are more highly correlated with sectors than with regions.

- In Latin America, the Middle East and Africa, roughly fifty percent of the sample saw the threat as having increased in the last three years. In the developed economies of Western Europe and North America, two thirds see the prevalence of fraud as the same or lower.
- In Latin America, 72% saw themselves as vulnerable to fraud and corruption, the highest of any region; and Latin America also recorded the highest concerns about money laundering and theft of assets. Yet Latin America also showed the least investment in background screening,

demand greater accountability from companies both inside and outside their country. Payments of any kind to an official to influence the contracting process; the use of a third party or lobbyist to negotiate extraordinary benefits; or any illegal acts committed by local representatives or agents of a United States company, even for the benefit of a third party, may mean trouble for the company, whatever the nationality, if they have operations in the U.S. or securities listed there.

This extraterritoriality has not just affected United States government actions. Interest groups, non-governmental organizations, and even other governments have started suing multinationals in the United States for damages incurred from fraud outside the country.

This increasingly complex legal framework has not appeared in a vacuum. Societies around the world are ever more demanding regarding the behavior of companies and their representatives, and are less tolerant

physical security, due diligences, IT security, audit committees, reputational monitoring, or whistleblower hotlines.

- The Middle East respondents showed the highest levels of concern about internal financial fraud, and also suffered most from it.
- The pattern is the same in Asia: in Asia’s emerging markets, concern over fraud is higher. In India, 49% see fraud as having increased; in China, 42%; in Japan, 33%. In both India and China, sixty percent see themselves as vulnerable to bribery and corruption; in Japan, the figure is only 10%.
- Central and eastern Europe saw fraud as a declining problem, overall, including Russia. However, there were some very specific concerns. Over 60% saw themselves as highly or moderately vulnerable to bribery and corruption, and the region also showed the highest levels of concern about vendor/supplier fraud and management conflicts of interest.

of corruption, tax evasion or the funding of extra-legal groups.

These conditions are creating greater awareness and care among senior executives in the United States when acquiring companies or entering into strategic alliances outside of their country. More and more businesses are also starting to see the importance of undertaking regular reviews of branches or subsidiaries in order to identify risks and vulnerabilities. These precautions are now essential for firms everywhere. A sin in one jurisdiction may lead to a penance paid in another – perhaps many times over.



Andres Otero is head of the Bogota office, Colombia. Having run his own risk consulting firm, he now helps conduct anti-money laundering, fraud and conflict resolution cases for governments and private companies. He previously held senior positions in the Colombian government, European Union and Inter-American Development Bank.



Culture, compliance and China

In *Riding the Waves of Culture*, cross-cultural business specialist Fons Trompenaars distinguishes between “universalist” and “particularist” cultural approaches to right and wrong.

The universalist says, “What is right can be defined and always applies”; the particularist says, “What is right depends on unique circumstances and the obligations of relationships.”

Trompenaars’ data and my own surveys of business students at Stanford and Beijing Universities place the United States and Europe squarely in the former camp, while China fits neatly into the latter. One could have an interesting discussion about why, including references to the West’s Judeo-Christian heritage versus China’s Confucian roots, but this is of little use to the Corporate Compliance Officer in Chicago trying to build a culture of compliance in Shanghai.

Carl Crow, an American advertising and marketing executive in Shanghai, wrote in 1937: “The Chinese employee may give the most complete loyalty to a small and personally conducted business, like mine, but the idea of any sort of loyalty to a corporation, whose owners are merely a name to him, is something that comes outside the scope of his philosophy.”¹ This describes a particularist mindset: individual loyalties lie not with a distant entity, even if it is putting bread on the table, but with family, friends, and close colleagues. My experience in China over the past 28 years has been similar. Employees of vendors have sent me to their competition for a better deal after I established a personal rapport via only a brief conversation in Chinese.

In student surveys, I give options describing how they might handle the discovery of a good friend and colleague embezzling corporate funds to pay for his ailing mother’s medical bills. Among Chinese respondents, 70% to 80% think that the

embezzler should return the money but the company not be informed. While 40% to 45% of Americans make the same choice, a similar number think that the money should be returned and the company told. In other words, for the majority of Chinese respondents, personal relationships trump corporate ones.

It does not help to make value judgments. These are true cultural differences that can be dealt with effectively only in an open, non-judgmental environment. A company cannot simply translate its compliance policy and processes into Chinese and assume they will have the same effect in Shanghai as in Chicago.

What’s a compliance officer to do?

First, do not try to change China. Despite a world war and a revolution, attitudes there have not changed much since Carl Crow wrote 70 years ago, so they will probably not do so during your tenure as Chief Compliance Officer.

Second, more than in the West, compliance starts at the top. In China leaders, by virtue of their station, are looked up to and emulated. From a compliance point of view, it is important for your China head to take a personal interest in compliance, and to be seen to lead the effort to establish a culture of compliance. He cannot leave it to the “compliance guys”.

Third, you cannot change China, but you can choose who works for you. Compliance starts with recruiting. What is the candidate’s background? Has he/she gone to school in the West? Has he/she worked for other companies that have a strong compliance culture? Why did he/she leave those companies? Have you sought references from previous employers? For senior managers or those with access to sensitive information, have you performed discreet, pre-employment background checks to see if there are ethical problems in their pasts? All these questions should

also be asked in the West, but too often the background check is a cursory check-the-box exercise. In China it must be taken seriously. The recruitment process is also an excellent place to start instilling the importance of compliance in your corporate culture. During the interviews and in written tests, some questions should probe the candidate’s views on ethics and compliance.

Fourth, try to establish a small company atmosphere even if yours is large. Chinese employees attach themselves more readily to those around them than to a corporate presence. Make sure department heads buy into the compliance culture and encourage them to develop a personal management style.

Fifth, set up a whistle-blower program. The Chinese have an old saying: “kill a chicken to frighten the monkeys.” Follow up on all reports of non-compliance and publicly deal fairly but sternly with instances of it.

Finally, compliance-related training and follow-up must be an integral part of the employee’s corporate life, even more than in the West.

The special challenges of compliance in China arise from cultural norms that are not subject to rapid change. While you cannot change the culture, an appreciation of it will let you take concrete steps toward a strong culture of compliance within your China business.

¹ *Four Hundred Million Customers*.



Frank Hawke is Chairman of Greater China and Southeast Asia based in Beijing. He has spent 27 years in China working as President of IMC Asia, Investment Banking head for Saloman Brothers and various other investment banks in China and Vietnam. He sits on the Board of Directors of China Everbright Bank. He has an MA in Political Science from Stanford University and is a visiting lecturer on Chinese Politics at Stanford University.

A proactive strategy for operational risk



Why has there been, in the last few years, extraordinary public and media focus on corporate governance and operational risk, specifically fraud? Recent corporate scandal is an obvious place to start – what happened at Enron, Worldcom, Tyco, and Parmalat was criminal, as the courts are showing – but is there another reason corporate governance is being pushed?

There are now more Mom and Pop shareholders than ever before and ordinary investors are wiser and shrewder with their money. They demand value and want a return. Recent questionable decisions by Boards have left these shareholders seeking answers and, in some ways, retribution for their losses. Recognition by politicians that these same investors are voters explains the growing interest in redressing grievances of this kind. This political pressure has led to increased severity in how regulators enforce the rules.

The problem with fraud is that its occurrence and form are unpredictable.

The introduction of enhanced corporate governance regimes should give the average investor, with relatively few means of influence, confidence in Board actions. Corporations are now being forced to do something about governance and operational risk: the United States has established some very onerous rules with the Sarbanes-Oxley Act; the Code on Corporate Governance Practices is being implemented across Asia; and the financial sector's governance is being further enhanced with the Basel II Capital Accord. These and other instruments are introducing substantial changes in how directors and Boards must operate.

So what can Boards do to improve governance with the aim of combating fraud and operational risk?

The problem with fraud is that its occurrence and form are unpredictable. Common risk management practice overlays controls throughout a function or process to minimize breaches. This works for standard situations but fraud breaks all rules. A fraudster seeks out and exploits weaknesses in an organization.

Boards can combat fraudsters with a fraud risk management strategy and Fraud Control Plan.

The tone for a robust fraud risk management strategy starts at the top. The media report large-scale fraud on a daily basis and yet most firms treat it as something that happens to other people, placing misguided trust in “all” staff members. Instead, a corporate culture that heightens and maintains awareness of fraud must be established. This can be achieved through training sessions, literature, and e-learning. The advantage of the latter is that it can provide valuable statistical information to organizations on the levels of fraud awareness that staff actually have.

Once the cultural tone is set, a company must build a framework for an overall Fraud Control Plan. The plan should include policies and procedures – including Codes of Conduct or Ethics – that must be communicated to, and adhered to, by all members of the organization. Employment screening is another key element in the plan: approximately one in four resumés has material errors or omissions. Whistle-blower policies provide an excellent source of information relating to misdeeds within an organization, although companies need to distinguish good information from the vexatious or malicious. For financial institutions, anti-money laundering and

account opening policies also form part of an overall Fraud Control Plan.

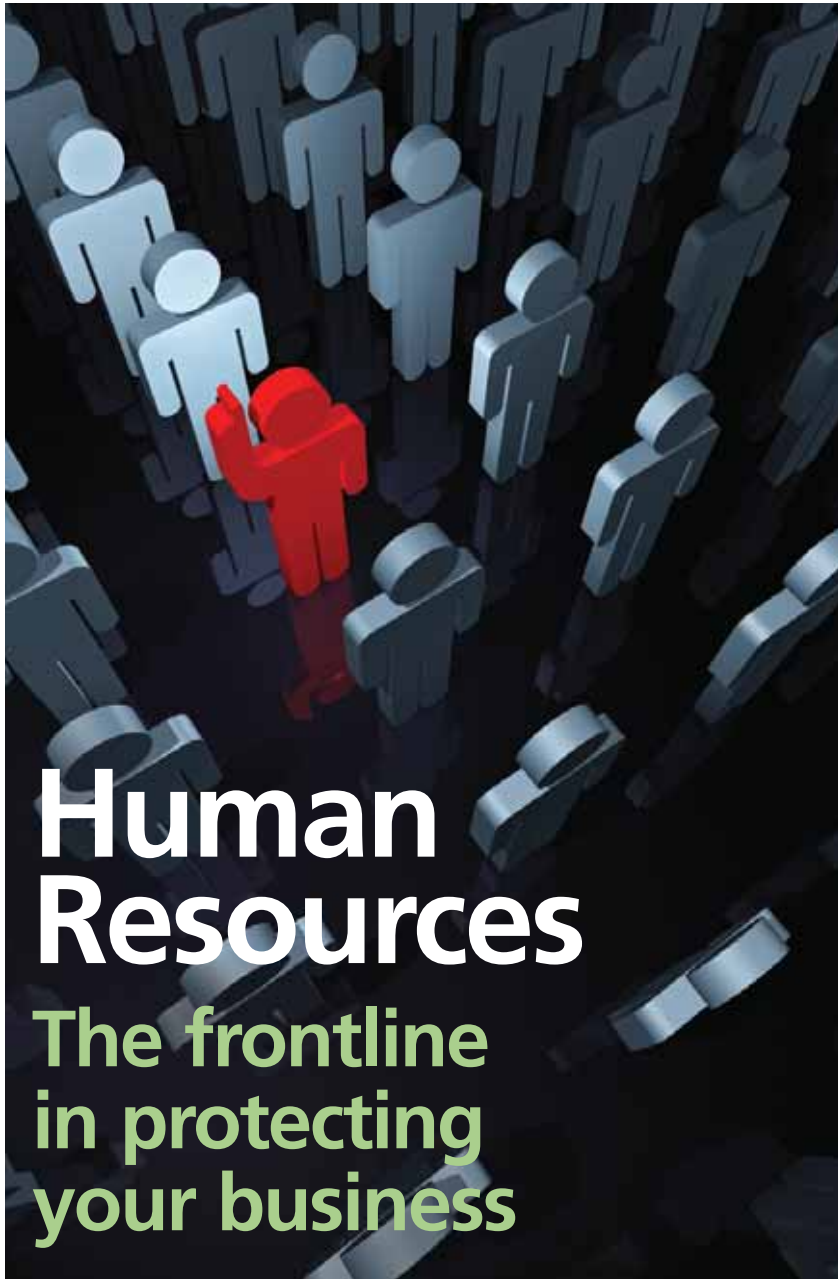
The next step in implementing a proactive risk strategy is to identify where the organization may be exposed. The U.S. Securities and Exchange Commission has not specified the exact framework to be used here, although it has indicated that it must be free from bias and permit reasonably consistent qualitative and quantitative measurements of a company's internal control environment. The framework on internal control suggested by the Committee of Sponsoring Organizations of the Treadway Commission is a good place to start. While this exercise can be complicated and time consuming, afterwards, the businesses will be in a better position to identify, analyze, evaluate, treat, monitor, and review fraud risk. The exercise also helps in meeting the rules and regulations of various jurisdictions and stock exchanges, as well as, for financial institutions, helping with Basel II compliance processes.

Finally, risk strategy must change with the organization, being continuously reviewed to insure that the controls that have been instigated are still effective.

Adopting a strategy along these lines places an organization in the best possible position to avoid the damaging consequence of fraud. It is also an indication to insurance companies, regulators, and investors that the company takes the issues of fraud and corporate governance seriously, thereby reducing costs and increasing access to capital.

Ferrier Hodgson offers a large and independent forensics service. With more than 50 dedicated specialists across Asia-Pacific, including a number of widely regarded experts, we have one of the region's most significant forensic capabilities.

 **FERRIER HODGSON**



Human Resources

The frontline in protecting your business

The human resources division of any organization should serve as its first line of defense in decreasing the risk of fraud. If organizations spend time and money up front screening prospective employees and also internal candidates for position changes and promotions, they will greatly decrease the potential for economic, reputational, and other types of injuries. While many job applicants may “embellish” their experience, skills, or responsibilities on their resume, others make blatant misrepresentations, fabricate college degrees and other information.

The time and expense of conducting a background search should be considered the cost of doing business that a company cannot afford not to incur. It will be time and money well spent in comparison to the consequences of not researching all prospective employees, or existing employees seeking to change positions within a company. Companies should also verify the backgrounds of candidates for all levels of responsibility, as even CEOs and other senior level executives have been known to falsify their resumes.

Sometimes the most obvious items such as education go unchecked which can result in embarrassment to an organization and obviously to the individual involved. A recent example of such an embarrassment comes from the academic world. Marilee Jones, the Dean of Admissions at MIT, one of the most prestigious and rigorous institutions in the United States and the world, resigned in April 2007 after MIT discovered that Jones had lied about her education. Jones was a 28-year employee of MIT, who had started as an administrative assistant, and worked her way through the ranks to apply for the Dean of Admissions position in 1997. Jones’ original resume represented that she had received degrees from three schools, when in fact she had received none of these. MIT did not verify her credentials at the time of her original hire, nor at the time she applied for the position from which she resigned. To add insult to injury, Jones was outspoken on the issue of “resume padding”, maintained a blog and spoke about the pressures on youth to exaggerate their accomplishments on their resumes.

Sometimes the most obvious items such as education go unchecked.

Such incidents also occur in the business world. In February 2006, David Edmonson, CEO of RadioShack, a NYSE-listed company, resigned after the company discovered that he had falsely claimed to have earned two college degrees. In reality, Edmonson had completed only two semesters of college. Edmonson was originally hired as Vice President of Marketing for a company subsidiary and although the company performed a background check it failed to verify his education. The company did not perform any updated or additional inquiries into Edmonson’s background when he was being considered for the CEO position.

In both cases, the lack of pedigree did not necessarily equate with lack of experience or qualification for those positions. And while these incidents did not necessarily result in direct economic injuries, they did result in great embarrassment and raised questions regarding both organizations.



Nancy Goldstein is an associate managing director for Latin America and the Caribbean. She specializes in securities and accounting fraud and market manipulation cases. She spent 17 years as an enforcement attorney for the U.S. Securities & Exchange Commission, NYSE and NASD.

Protecting your investments



Stop and think for a moment about how many companies all around the world are right this minute looking at a huge opportunity to grow, either through merger, acquisition, or joint venture. A good part of these opportunities may seem irresistible and, in the business world, speed is of the essence. It is precisely within this context that proper due diligence is overlooked.

In general, there are three types of due diligence: financial, legal and reputational. The first checks the accuracy of the financial statements, as well as the financial health of the target company, including an analysis of its assets and the origin and destination of its funds. The second does the same for legal aspects. Reputational due diligence explores the background and market image of the company with which one wants to do business. This includes its corporate culture and its reputation with employees, investors, consumers, the press – all groups that are directly or indirectly part of the market chain.

Proper due diligence is obviously important. Many companies, however, only become aware of how important after the fact, especially when they conduct a reactive process to see if there are grounds for suspicions.

In addition to protecting companies considering an investment, due diligence can be a very efficient fraud prevention tool. As experience is always the best teacher, consider the example of XPITO (a

pseudonym for a real company which had just acquired a smaller firm).

One of XPITO's executives suspected that the inventory recorded under assets was significantly overstated. He accordingly conducted a reactive due diligence process that confirmed his suspicions. The subsequent investigation revealed that the Vice-President of Finance of the acquired business, an employee with over five years of service, had been stealing goods and selling them to the competition, covering up his wrongdoing by falsifying the company's inventory control records. An in-depth assessment of the company's internal controls revealed serious failures that left it vulnerable on several fronts. The question that immediately arose, of course, was if this had been the first case of internal fraud.

Often fraud is committed by people who have been with the company for years, never go on vacation and are well trusted.

Time showed that it had not. Almost one year after the acquisition, it became apparent that the Commercial Director of the acquired company owned a competing business, in direct violation of XPITO's policies and rules of conduct. The first

“smoke signal” was in an anonymous fax to the CEO, who decided to investigate the case immediately. The investigation revealed that the Commercial Director had a lifestyle far above what would be reasonable based on his income from XPITO. Further investigation showed a fully operational competing business, registered in the name of the executive's spouse to prevent suspicions. Even more disturbing, the Commercial Director was a trusted employee who had been with the organization for about 10 years.

Kroll, in its more than three decades of conducting investigations, has found that that often fraud is committed by people who have been with the company for years, never go on vacation, and are well trusted. Companies considering a transaction therefore must include background checks in the due diligence process. The results can be surprising and will serve as a powerful fraud prevention tool, avoiding a lot of headaches.

As the CEO of XPITO later told us, “the next time we consider an important acquisition, we will check the barn before we close the doors.”



Vivian Bialski is head of marketing & communications for Latin America. Based in Brazil she has provided marketing and communication support in New York and across Latin America for eight years. Prior to this she coordinated internal and external communications projects at Vasp and Votorantim.



Up to the top: Financial statement fraud

Fraud at companies such as Enron and WorldCom led Congress in 2002 to pass the Sarbanes-Oxley Act, which tightened reporting requirements for companies and increased penalties for financial crime. Despite stringent legislation aimed at combating financial fraud, however, it remains a public concern. Why, then, does financial statement fraud occur?

Motivating Factors

Robert Tillman and Michael Indergaard recently described various factors which produce this fraud, including: a desire by firms to meet earnings estimates or to raise funds from capital markets at low costs; Boards having fewer outside directors, making them more likely to manipulate earnings; the presence of certain performance-based executive compensation which is more susceptible to fraud; and insider trading. The authors also tied the flood of financial statement fraud to larger changes in the economic environment, business organizations, and corporate culture. For example, after the deregulation of the 1990s came the evolution of “network structures”: flexible relationships between firms “in which business [became] increasingly organized around ‘deals’ and ‘deal flows’,” as well as the further development of “reputational intermediaries” – such as banks, law firms, or accounting firms – that assisted in the financial engineering of deals. The result was an environment ripe for the execution of financial fraud. According to Tillman and Indergaard, these changes normalized

criminal behavior in business, as executives were encouraged to engage in corrupt activity to complete deals and audit firms turned into consultancies driven by revenue generation.¹

Types of Financial Fraud

This research finds three basic types of financial fraud: isolated, perpetrated by senior management cliques, and boundary-crossing. In all of these, CEOs may be involved. According to the General Accounting Office, between January 1, 1997 and June 30, 2002, they were named in nearly 90% of the class action suits and Securities and Exchange Commission actions filed as a result of restatements.²

The characteristics of the categories are as follows:

Isolated: Isolated frauds involve only one or two senior managers executing simple embezzlements or revenue manipulation, such as the U.S. Wireless case in which the former CEO and General Counsel diverted millions in stock and cash into personal off-shore accounts. They tend to be revealed quickly because the managers operate with little or no assistance from their peers.

Senior Management Clique: These involve a number of senior managers colluding to manipulate financial results, with CEOs and CFOs often heavily implicated. According to Tillman and Indergaard, the “collective mustering of the information advantages and institutional levers” exercised by these managers greatly extends how far these frauds can go.

Boundary-Crossing: In these cases, senior managers use their influence and informational advantages to draw mid-level or senior management from outside firms into the collusion, such as in the Homestore case in which senior managers allegedly enlisted mid-level managers both from within their own firm and from outside firms in order to deceive the auditors. As in senior management clique cases, CEOs and CFOs tend to be heavily involved.

Overall, one leading cause for any financial statement fraud is a corrupt CEO. However, inadequate internal controls and an ability to deceive outside auditors also contribute. Although further legislation will not stop financial statement fraud, the requirements of Sarbanes-Oxley have significantly increased the attention paid by management, Boards of Directors, and auditors to corporate governance and to internal controls and financial reporting. This has helped improve the quality of these controls and deter fraud, which should, in turn, continue to boost investor confidence.

¹ “Control Overrides in Financial Statement Fraud”, Report to the Institute for Fraud Prevention. (2007)

² Financial Statement Restatements: Trends, Market Impacts, Regulatory Responses, and Remaining Challenges. (2002)



Doug Farrow is a managing director in Los Angeles. He has over 20 years of experience dealing with accounting irregularities and litigation related to financial issues. He previously worked at KPMG and serves as an expert witness and arbitrator. He is a Certified Fraud Examiner (CFE) and CPA.



David Hess is a managing director in Washington. He has more than 20 years of experience providing forensic accounting, auditing and consulting services in both government contracting and commercial arenas.

Protecting data sources from internal theft

According to the 2006 CSI/FBI Computer Crime and Security Survey, the four most expensive computer crimes, accounting for 74% of losses, are: viruses, unauthorized access, laptop or mobile hardware theft, and theft of proprietary information.

For many organizations, proprietary information is a critical asset and can cost companies millions of dollars if stolen. While companies frequently take precautions to defend against outside threats to their intellectual property, including hackers and so-called “malware” – computer viruses, worms and Trojan horses – they also need to consider potential internal threats – the disgruntled employee, the well-meaning but misguided one, the quasi-employee, workers at firms receiving outsourced work, and simple human error.

Employees are already inside firewalls, intrusion detection systems and other forms of IT security.

Employees are more likely to engage in such theft than external hackers because the former have nearly unfettered access to a company’s sensitive data. In addition, employees are typically already inside firewalls, intrusion detection systems, and other forms of computer security. In fact, according to *The Global State of Information Security 2005* from PriceWaterhouseCoopers and *CIO Magazine*, former employees and their partners committed 28% of information security attacks; internal employees committed 33%.

Therefore, an effective information fraud interdiction program must encompass everyone with access to proprietary information, not just employees, but part-timers, temporary service workers, and employees of outsourcing companies that handle sensitive data. The program should deploy tools that can deter, detect, defeat, and document problems, whether the result of malice or error: for example, the



employee who suddenly starts exporting sensitive information should raise questions. Just as important as technical safeguards are training and defined processes to provide consistency in the use, storage, and disclosure of sensitive information.

Often disgruntled employees are involved in information security incidents. Corporations, in establishing or reviewing their information protection arrangements, should consider the following methods of data transfer frequently used by employees:

- **Email:** Eight out of ten employees admit to sharing confidential information with other companies via email;
- **Instant Messaging:** Without preventative controls, employees can use IM tools to transfer files and send small amounts of text.
- **CDs or DVDs:** Gigabytes of data can be transferred to these discs in minutes;
- **Digital Cameras:** Devices of all sizes now have digital cameras, allowing an employee to take pictures of highly sensitive areas or documents. When connected to a computer through a USB port, they can also receive multiple gigabytes of data by simple file copying;

- **Other Small Data Storage Devices:** Personal Digital Assistants – iPhones, Palm Pilots, BlackBerries, and PocketPCs – can be used to carry data covertly out of an organization. USB drives are typically the size of a tube of lipstick and so pervasive that even Swiss Army Knives and key rings have been fitted with them. These provide almost unlimited storage to take information out of a corporation quickly, quietly, and discreetly. For those needing more, an external hard drive with a USB connection and capacity of 160GB costs less than \$100;
- **Radio-based gadgets:** Wireless routers and networks, and Bluetooth dongles – which allow you to connect a cell phone or PDA to a computer – multiply the threat.



Alan Brill is a senior managing director and specializes in communication security and technology crime response. He previously held the position of Director of the Information Systems and Information Security Bureau at the New York Department of Investigation. He serves on the Board of Advisors for the Center for International Financial Crime Studies at the University of Florida’s Levin School of Law and is an Adjunct Professor at National University in San Diego. He is a Certified Fraud Examiner (CFE) and Certified Information Forensics Investigator (CIFI).

Making employee hotlines work



All too often, preventable frauds occur because employees with suspicions lack any effective mechanism through which to share them. A confidential reporting channel for employees, suppliers, and others is an excellent and very useful tool to improve fraud detection.

Many international surveys of fraud, and Kroll's own experience, make clear that the most effective means of uncovering fraud is the "tip off". Each year, our investigators receive anonymous letters, emails and messages indicating possible fraud. Perhaps more interesting, however, is that these "tip offs" are frequently not reported through existing channels, such as whistle-blower lines. In fact, of the many frauds we have detected, the investigation has rarely begun after a report on a company hotline.

The most effective means of uncovering fraud is the tip-off.

Why is this? Many employees do not believe that such mechanisms will make a difference. They are often scared of personal repercussions or are bound by a culture of *omertà*, which holds that the worst thing you can possibly do is to implicate your fellow worker. Some even believe that the lines form part of senior

management's conspiratorial schemes to protect themselves. Establishment of reporting mechanisms is fundamental in fighting fraud, but simply hoping that the good, honest employees will call is wishful thinking. A successful reporting line requires constant hard work.

Here are a few dos and don'ts:

Do:

- Make a reporting line part of a wider, positive integrity program that will review and update existing company policies and demonstrate support from the top. Individuals do not like to suspect people or organizations with which they have a relationship, but it is critical that the employees see reporting suspicions as not only their obligation but also in their own interests. For example, if money is successfully recovered from a fraud, then give the users of the reporting line some of it, or agree that for every report received the company will donate something to a local charity;
- Link the policy into the local culture of the employees;
- Involve trade union representatives with the scheme. Without their support workers will have another reason to feel reluctant to use it;
- Make a substantial effort in advertising. Use company intranets, posters, training programs;

- Insure that all reports are handled sensitively. When fraud is alleged, there is a two-way obligation. The first is to the company to preserve its position and reputation. The second is to the person against whom the allegation is made, who must be positively cleared or exposed. The worst outcome is for a cloud of suspicion to hang over an honest person;
- Train specialist teams in both Audit and Security to handle the reports or even outsource management of the whole system to an independent third party;
- Insure that strict disciplinary action is taken against those found to abuse the system.

Do not:

- Delay when suspicions are aroused. This allows perpetrators to seize the initiative and prevents allegations from being professionally investigated;
- Discuss suspicions with anyone who does not need to know;
- Allow employees to investigate suspicions without reporting them. This may, in the process, alert perpetrators that they have been detected.

Charles Carr is a managing director and head of Fraud for Europe, Middle East and Africa. He was previously head of the Milan office and country manager for Mexico and specializes in fraud presentation programs and training. He previously spent time as an oil futures broker for Kidder Peabody.

Investigative tactics under scrutiny in the United States



The past year has seen a spate of news stories about overzealous investigators getting into trouble, sometimes along with the lawyers who hired them. An era of heightened scrutiny is upon us. Although both in-house and outside counsel frequently rely on private investigators to unearth difficult-to-find information, they should assume that the investigative strategies used might ultimately be scrutinized by law enforcement agencies. By knowing which of these are legal and ethical and those which are illegal, counsel can evaluate strategies proposed by private investigators and draw the line at inappropriate or unwise methods.

In an investigation that went notoriously wrong, private investigators seeking a source of media leaks for Hewlett Packard impersonated board members and journalists in order to obtain confidential telephone records. The result was criminal charges filed against the company chairman, its in-house compliance lawyer and the investigators. Hollywood investigator Anthony Pellicano also faced federal criminal charges for allegedly bribing a police officer and a telephone company employee to provide him with confidential information and for installing wiretaps on the individuals he was hired to investigate. A prominent Los Angeles attorney who had hired Pellicano, Terry Christensen, was also indicted.

Avoiding such a fate requires, above all, hiring a firm with a reputation for, and record of, ethical conduct and conducting a full and frank discussion on strategy and tactics. In many cases relevant laws are

obscure or ambiguous. It is not always a case of plainly illegal conduct, but rather of “I didn’t know you couldn’t do that.” Counsel should be especially alert to legal and ethical considerations in the following areas.

Electronic Evidence

The first step in many internal investigations is to gather and analyze evidence from a variety of electronic sources at the company in the U.S. Most company codes of conduct make it clear that employees can have no expectation of privacy for data, even personal data, present on company computers or servers. To avoid any later lawsuit, however, it is prudent to review company policies prior to looking at such data. Ideally, the code of conduct or the employee manual should unambiguously state that all messages and data generated from, received on, or stored on company equipment are company property.

Telephone Records

These can also be a fruitful source of evidence, but investigators will generally be limited to obtaining the records of company landline phones and cellphones. If an investigator claims that he can obtain private telephone and financial records, it should be a huge red flag and the supervising lawyer should closely question the process involved. Obtaining such records through “pretexting”, posing as the subscriber in order to fool the phone company into divulging information, was a principal source of the trouble in the Hewlett Packard case. The recently enacted federal Telephone Records and Privacy Protection Act, as well as new state legislation have addressed this issue directly, including with criminal penalties for those whose tactics fall on the wrong side of the law.

Surveillance

Surveillance is another classic investigative tactic that must be used carefully. Silent video surveillance is legal in some states, unless occurring where the subjects have a reasonable expectation of privacy. Laws on audio surveillance, such as tape-recording a telephone conversation, vary from state to state. Most require the consent of only one party to the conversation, but some demand consent of all parties. Physical surveillance, such as staking out a location or following the target around, is legal as long as the investigator remains in public areas and the surveillance does not

constitute an overt effort to intimidate, also known as “rough shadowing.” Even though such tactics are permissible, a lawyer supervising an investigator should weigh the potential negative consequences should the activity become public. Hewlett Packard, for example, was sharply criticized in the press for “spying” on members of its Board and reporters.

By taking these steps and understanding the tactics involved, counsel can help to both develop an effective investigative strategy and make sure that the tactics used do not come back to haunt the company.



Andrew Cowan is a managing director in Los Angeles specializing in complex internal investigations and litigation support. He previously served as assistant U.S. attorney in Los Angeles in the Public Corruption and Government Fraud section and as a trial attorney for the U.S. Department of Justice’s Antitrust Division in Washington DC.

Who is taking responsibility for losing sensitive data?

In the past several years, hundreds of companies have suffered from security breaches that negatively impacted their reputation and economic future. Ignorance of unrecognized weak spots is no defense. Today, organizations and individuals worldwide are acutely aware of what happens after learning that sensitive information has been compromised – no matter whether it was improperly stored on a missing laptop or accidentally tossed into a garbage bin.

People who feel thrust into jeopardy by a company’s mishandling of their sensitive data will not hesitate to show displeasure. As an online columnist wrote after discovering his own name in a third-party breach of hotel data, “Now it’s personal. Now I’m angry.” One 2006 survey of consumers in this position indicated that almost 60% had severed or considered severing their relationship with the privacy-offending company. Research conducted with organizations that had experienced a breach revealed that 74% of them had lost customers.

Whether companies succeed or fail to maintain business and brand loyalty in the wake of a data loss may be directly attributed to how they treat and protect affected individuals. As public knowledge about identity theft and fraud grows, so do expectations that companies step up to the plate.

Consumers whose personal details have been exposed typically react with anger and then uncertainty. They want reassurance that the company is taking responsibility. They want to understand what happened. They want to talk with someone about it. But most of all, they want to know what is going to be done to counter the effect this may have on their lives.

The obvious solutions are not enough to suggest that someone in this position “contact one of the three credit reporting agencies” disregards the majority of the risk they face. The U.S. Federal Trade Commission reports that less than 24% of identity theft is revealed by credit-related data. Moreover, data repositories are not known for providing upset callers with easy access to customer service experts who can calm nerves or offer help with what to do next.

Blanket recommendations to “file a fraud alert or secure a credit freeze” leave that same gap. Besides, neither a fraud alert nor a credit freeze can stop check fraud, tax fraud or sale of stolen identities for cash or drugs.

While “credit monitoring” generates an alert when suspicious activity occurs, privacy breach victims are frequently left to fix the problem themselves, with no support.

Elements of Best Practice

Companies interested in retaining loyalty, reputation, and share value differentiate themselves by offering solutions such as identity theft restoration. True restoration solutions give individuals access to experts who understand what has happened, know what needs to be done and can take most of the burden off the victim’s shoulders to restore an identity to pre-theft status.

Following the trail of identity fraud beyond credit-related data and into a potentially complicated landscape is no job for marketers or “advocates” without a risk or security management background. A credentialed team of licensed investigators, working with the victim’s permission, knows where to look and how to recognize fraudulent activity, and is more likely to employ security industry resources that might otherwise be unavailable. Licensed investigators work with the victim until the stolen identity is restored to his or her satisfaction, no matter how long it takes.

Damage from identity fraud associated with a data breach can be expensive, for both the breached company and the people whose data was lost. Response plans that demonstrate accountability and put the affected individual’s best interests first are critical to restoring trust and reclaiming consumer confidence.

Brian Lapidus is a senior vice president based in Minnesota. He leads a team of investigators in ID theft discovery, investigation and restoration including helping corporations to safeguard against and respond to data breaches.

U.S. Government increases controls over contractors



The United States Government is increasing action to address fraud against itself in a variety of ways.

The U.S. Department of Justice (DOJ) recovered \$3.1 billion in connection with fraud and false claims actions in 2006, a record for a single year. Of these, 72% occurred in health care, 20% in defense, and 8% in other areas such as disaster assistance and agricultural subsidies. Suits brought by whistleblowers under the False Claims Act – which lets individuals file on behalf of the government against those who have defrauded it and share in any funds recovered – accounted

for \$1.3 of the \$3.1 billion. Accordingly, whistleblowers received \$190 million in 2006. Attorney General Alberto Gonzales claimed that “these recoveries send a clear message that the Justice Department will not tolerate fraud against the government. Since 1986, the Department of Justice has recovered \$18 billion from those who commit fraud.”

Barry M. Sabin, Deputy Assistant Attorney General for DOJ’s Criminal Division, appearing before a Congressional committee, reiterated the department’s “commitment to a strong and vigorous enforcement effort.” He added that DOJ has

Profiting from stolen information

No one would think of leaving a factory unlocked at night, yet few companies have as effective controls on their information assets as they do on their physical assets. More and more, Kroll gets asked to help clients who have had confidential information stolen – information which in unauthorized hands can cost them millions of dollars.

In the last year, these cases have ranged from pricing information in a multi-million dollar bid to proprietary software and client lists. Each time the data was taken with the intention of inflicting commercial damage on the rightful owners, and often to make money for the thieves. In one case, a company worth millions of dollars had left its key information database open to all employees – without even basic password protection.

Advances in the storage capacity of small USB memory sticks mean that large volumes of data can leave a company in an employee's pocket. In one recent case, a disgruntled employee took confidential financial information home on his iPod. While good information-security procedures can make information theft more difficult, the range of ways information can be relayed means that such prevention can never be complete.

The work of retrieving stolen information, however, and of recovering damages, is made much easier if companies have at least observed the following:

- Insure that IT staff routinely record and retain logs of activity on company data servers, despite the marginal loss of performance that results;
- Make clear in employee contracts, company IT policies or employee handbooks that the employer has the explicit right to monitor emails for the purposes of preventing or catching wrong-doing. Also, make it clear that corporate equipment – including computers, cellphones, PDAs, and similar devices – remains company property even if it contains personal data;
- Keep itemized number-called logs of telephone calls made from office phones and corporate cellphones;
- Consider the use of CCTV on office exits and entrances, and the use of security card-controlled doors in areas where confidential information is stored.

The good news is that if stolen information is valuable, it will be used somewhere and is likely to come to the attention of the company from which it is taken. A business

It is possible for investigators to look quickly for key digital fingerprints left by thieves.

should act quickly if it learns of such a theft, or becomes suspicious that one is about to occur – perhaps by employees who intend to set up their own rival business. Server logs, laptops, cellphones, PDAs and other potential sources of evidence should be secured.

It is possible for investigators to look quickly for key digital fingerprints left by thieves. Computers contain information about web mail accounts, often used to send information out of companies. Data mining techniques can be used to analyze thousands of phone calls or emails for tell-tale clues. Surveillance of the key suspects can reveal potential buyers or backers. Typically, with some initial evidence, interviews with staff and suspects will unravel details of the scam. Fellow workers may have noticed something strange, the suspects may have bragged at work or at home, or simply made a mistake in covering their tracks. In other cases, with sufficient prima facie evidence of wrongdoing, courts can be persuaded to allow the search of residential property or seizure of financial records to yield clues.

Sometimes the investigation may even reveal that things are not as bad as they seem. A credit card company engaged Kroll to retrieve a missing hard drive which contained important details of all its customer accounts. The appropriate regulatory authorities were duly informed. The worst-case scenario was that an organized crime group had stolen the data to use in perpetrating identity frauds. Meticulous questioning of all those who had come into contact with the hard drive, combined with computer forensic evidence showing access, eventually led us to the thief. Why had he stolen the hard drive? He had run out of computer memory to record the TV series *Lost* and had taken it for that purpose. The valuable personal data? Deleted.

Benedict Hamilton is a senior director based in London. He works on fraud and financial mismanagement investigations and loss recovery. Previously he spent 12 years working as an investigative journalist for the BBC and Channel 4 and was twice nominated for RTS journalist awards.

made the investigation and prosecution of procurement fraud a priority and that it is working through a specialist government agency to investigate such fraud relating to the wars and rebuilding efforts in Iraq and Afghanistan. Sabin also stated that, in order to leverage law enforcement resources and more effectively investigate and prosecute procurement fraud, DOJ had formed the National Procurement Fraud Task Force.

This action, in October 2006, was a significant step in the government's war on fraud. The Task Force's purpose is to "promote the early detection, prevention, and prosecution of procurement fraud associated with the increase in contracting activity for national security and other government programs." The body includes the FBI, multiple federal agencies' inspectors general, defense investigative agencies, federal prosecutors, and DOJ divisions. It is emphasizing increased civil and criminal enforcement in areas such as defective pricing, product substitution, misuse of classified and procurement-sensitive information, false claims, grant fraud, fraud involving foreign military sales, ethics and conflict of interest violations, and public corruption associated with procurement fraud. Since its formation, more than 150 procurement related fraud cases – although not all stemming from its work – have resulted in criminal charges, criminal resolutions, or civil settlements.

Two amendments to the Federal Acquisition Regulation have also been proposed recently to assist in the fight against procurement fraud. One would require contractors to establish and maintain internal controls to detect and prevent fraud in connection with their contracts, and to notify contracting officers promptly if they become aware of a contract overpayment or fraud. The second would require contractors to have an effective compliance and ethics program.

It is evident that the government will continue to combat fraud through a concerted and coordinated effort. Accordingly, it is likely that the substantial monies spent in the war on terrorism in recent years, along with other initiatives, will be targets of government fraud investigations.

James Check is a managing director based in Washington. He specializes in government contractor advisory services having previously spent 16 years at Arthur Andersen, five as partner. He is a CPA and member of the AICPA.

Gary Adams is a director based in Washington. He has over 25 years of experience of federal compliance and budget preparation oversight. Previously he was vice president of FAR compliance services. He is a CPA.

North America

Consulting Services

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

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

Kroll Ontrack

Tony Cueva
Minneapolis
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
1 305 789 7100
sanson@kroll.com

Eduardo Gomide
São Paulo
55 113 897 0900
egomide@kroll.com

Asia

Consulting Services

Tadashi Kageyama
Tokyo
81 332 184 558
tkageyama@kroll.com

Anne Tiedemann
Hong Kong
852 288 477 88
atiedemann@kroll.com

Kroll Ontrack

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

Europe, Middle East & Africa (EMEA)

Consulting Services

Charles Carr
London
44 207 029 5000
ccarr@kroll.com

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

Kroll Ontrack

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

Identity Theft

Toni Sless
London
44 207 029 5077
tsless@kroll.com

Background Screening

Michael Whittington
London
44 127 332 0060
mwhittington@kroll.com

Headquartered in New York with offices in more than 65 cities in over 33 countries, Kroll has a multidisciplinary team of more than 4,200 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. We design solutions to your problem – be it global, local or cross-border 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
- Corporate Advisory & Restructuring
- Data Recovery & Legal Technologies
- Business Intelligence
- Hostile Takeover, M&A and Hedge Fund Intelligence
- Employee & Vendor Screening
- Valuation Services

KROLL

