



Global Fraud Report

Global and local issues
discussed.

Sector by sector analysis.
Economist Intelligence
Unit analysis.

Correction


In the July 2008 issue of the Global Fraud Report the article "Written or oral reports? Don't waive your rights accidentally" was incorrectly attributed solely to Asuncion C Hostin. The article was primarily written by Gilbert Boyce, litigation partner at Kutak Rock and should have been attributed to him accordingly.



Gilbert Boyce is a partner in the litigation department of the Washington, D.C. office of Kutak Rock. He has been lead trial or appellate counsel for brokerage firms, financial institutions, insurance companies, non-profit organizations, and accounting firms in a wide range of complex litigation in federal and state courts, the U.S. Tax Court and before various arbitration tribunals.

Global Fraud Report

| | | | |
|--|----|---|-------|
| INTRODUCTION | 5 | RETAIL, WHOLESALE & DISTRIBUTION | |
| Ben Allen, President & CEO..... | | Profile: Leading express and mail provider shows the way..... | 22 |
| EIU OVERVIEW | 6 | Reducing retail fraud through background screening..... | 23 |
| The Economist Intelligence Unit overview..... | | VIEWPOINT | |
| FINANCIAL SERVICES | | How quickly can you detect a data breach? How will you respond?..... | 24 |
| Hazards in hedging contracts..... | 8 | CONSUMER GOODS | |
| Benefits of detection..... | 9 | Using the International Trade Commission in IP investigations..... | 26 |
| PROFESSIONAL SERVICES | | VIEWPOINT | |
| New rules cause law firm problems..... | 10 | Word Power: Linguistic analysis assists fraud investigations..... | 28 |
| VIEWPOINT | | TRAVEL, LEISURE & TRANSPORTATION | |
| Protective steps in internal public company investigations..... | 11 | Common scams in hospitality..... | 28/29 |
| MANUFACTURING | | CONSTRUCTION | |
| The risks keeping manufacturers awake at night..... | 12 | Fixed-budget projects: hidden risks..... | 30 |
| HEALTHCARE, PHARMACEUTICALS & BIOTECHNOLOGY | | FRAUD VULNERABILITY | |
| Preventing data breaches in healthcare..... | 14 | Blowing hot and cold: Targeting areas of high risk..... | 32 |
| Strengthening information security..... | 16 | KROLL CONTACTS | 34 |
| TECHNOLOGY, MEDIA & TELECOMS | | KROLL SERVICES | 35 |
| The changing face of online brand abuse..... | 18 | | |
| NATURAL RESOURCES | | | |
| Guidelines for expanding in developing countries..... | 19 | | |
| VIEWPOINT | | | |
| Compliance: It's just good business sense..... | 20 | | |



Kroll commissioned The Economist Intelligence Unit to conduct a worldwide survey on fraud and its effect on business during 2008. A total of 890 senior executives took part in this survey. A third of the respondents were based in North and South America, 30% in Asia-Pacific, just over a quarter in Europe and 11% in the Middle East and Africa.

Ten industries were covered, with no fewer than 50 respondents drawn from each industry. The highest number of respondents came from the professional services industry (16%) followed by financial services (13%) and technology, media and telecoms (11%). A total of 42% of the companies polled had global annual revenues in excess of \$1billion.

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

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

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

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

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

Introduction



Ben Allen is president and chief executive officer of Kroll, based in New York. Prior to this appointment, Ben served as president of Kroll Technology Services, which includes Kroll Ontrack, Kroll's legal technologies & data recovery subsidiary, background screening and related services. Early in his career, Ben worked for Ceridian Corporation and 3M in sales, marketing, and management positions. He earned his B.A. in business from Washington State University.

I am delighted to welcome you to the second annual Kroll Global Fraud Report. As CEO of Kroll, the publication of this report each year is an opportunity to look beyond our day-to-day concerns, back over the work we have done, but also forward to the challenges that lie in the future.

When people think of fraud, I think many of us imagine the classic scenario of the staff member that disappears with the petty cash, or rogue traders on Wall Street, or pump-and-dump stock schemes. These certainly form a large part of the work we do at Kroll. Financial fraud – embracing all these and more – is a critical problem for many companies.

But as this annual issue of the Kroll Global Fraud Report shows, there is more to fraud than this. Information theft and threats to intellectual property are rising fast up the list of concerns. And the work we do increasingly focuses on these types of fraud.

Why should this be so? Partly, it reflects the ease with which criminals can make use of new techniques, gaps in infrastructure and the difficulties in resolving security issues with new software.

But it also reflects a change in the nature of business. It is a mistake to look at fraud only from the point of view of the threat. The biggest issue is the assets at risk, and the assets that companies guard most closely are increasingly held electronically: client data, details of how a product is manufactured, information on staff, new software, entertainment products... the list is endless. New technologies make these easier to produce and store; but sometimes easier to steal, and easier to resell.

My background is in our technology business. Kroll Ontrack has grown exponentially through data recovery, computer forensics and electronic discovery. At every stage we have worked with our colleagues in Business Intelligence

and Investigations as they increasingly sought the most up-to-date technology to find electronic evidence that could make the difference between success and failure in a complex case. In the last few years, both our groups have worked with our colleagues in Background Screening to produce solutions for ID theft, from breach protection, risk assessment, and planning to post-event response, customer notification, investigation, and resolution.

Increasingly, the work we do moves between accounting, investigations and technology. Few fraud cases involve only one element, and more and more of our work is genuinely global, involving cases in more than one jurisdiction. Products stolen in one country may be offered in a second for sale; the proceeds may go to a third country, and be banked in a fourth. The criminals may live in a different jurisdiction altogether – perhaps even on a different continent.

Some of the challenges we face in every fraud case are technical: how to use our technology to search Japanese characters, or the right ways to liaise with law enforcement, or where to find company registration details. But some of them are cultural: putting together multinational, multi-capability teams is complex and we learn more every year about how to do that. We pride ourselves on having the right people to address the most complex issues, and that means staying one step ahead of the fraudsters – but also keeping in touch with the way our clients do business.

I hope this report provides some useful food for thought.

A handwritten signature in black ink, appearing to read "Ben F. Allen".

BEN ALLEN

Economist Intelligence Unit overview



Fraud is a fact of corporate life. But the threat, and the way companies tackle it, changes over time. Kroll accordingly commissioned its second annual survey from the Economist Intelligence Unit of nearly 900 senior executives worldwide, 46% of whom are C-level executives such as CEOs, CFOs and CIOs, to obtain an accurate impression of the challenge fraud is presenting today. The key findings include:

Fraud, and vulnerability to it, is already widespread and increasing according to a variety of metrics:

- **Average Loss:** The average company in our survey lost \$8.2 million¹ to fraud over the past three years. This is up 22% from last year's survey when the figure stood at \$6.7 million. Larger companies – those with annual sales over \$5 billion –

lost nearly three times as much as the average, some \$23.3 million. Smaller firms suffered much less in absolute terms. Nevertheless, their loss per company, \$5.5 million, represents a 70% increase from last year's average.

- **Overall Incidence:** 85% of companies were affected by at least one fraud in the past three years, up from 80% in our previous survey. For larger companies,

the proportion is 90%. There is little room left for this figure to grow.

■ **Specific Fraud:** Only two of the ten categories of fraud tracked in the survey – money laundering and procurement fraud – declined in incidence for surveyed firms between last year's survey and this one, in each case by just 1%. Much more common were small but noticeable increases. For example, theft of physical assets, the most widespread fraud in both surveys, affected 37% of companies in recent years, up from 34%; information theft went from 22% to 27%; and regulatory and compliance breaches from 19% to 25%.

■ **Perceived vulnerability:** Again, with few exceptions, the number of companies considering themselves at least moderately vulnerable to each category of fraud rose, usually by about 5%. Seven in ten now believe themselves exposed in this way to information loss or attack, and just over one half think the same for regulatory and compliance breaches (54%), management conflict of interest (53%), financial mismanagement (52%), procurement fraud (51%), and physical theft (50%).

Weakening internal controls and high staff turnover both induce much higher levels of fraud than other risks.

Other risk factors have less of an impact. Poorer controls and frequent employee changes both significantly increased the frequency with which companies suffered from a range of frauds. [see chart]

Weaker controls – to which one-quarter of companies admitted – had a particularly striking effect, in almost every case increasing the proportion of companies hit by at least one-and-a-half times. Other factors which raised exposure, including entry into riskier markets, participation in joint ventures, and complex information technology (IT) arrangements, had much smaller overall effects, although these could noticeably increase the likelihood of certain types of fraud. IT infrastructure complexity, for example, correlates with a higher rate of information theft (32%) and intellectual property (IP) theft (21%), as does participation in joint ventures (32% and 24% respectively). Money saved on poor controls and low wages might well be lost to fraud.

Fraud is most prevalent in less developed economies. Overall, the more developed economies – North America and Western

Europe in particular – have seen less widespread fraud activity, while the economically less developed ones – notably those in the Middle East and Africa – have experienced much more. In eight out of ten fraud categories, the latter region had the highest or second highest incidence of activity, and in the same number of cases North America had the lowest. The only marked exception was intellectual property theft, in which less developed regions had the least, and North America actually had the most occurrences.

Economist Intelligence Unit

¹ Estimate based on weighted averages



Percentage of companies suffering from fraud in past three years

| | Overall | High Staff Turnover | Weaker Controls |
|---------------------------------|---------|---------------------|-----------------|
| Corruption/Bribery | 20% | 23% | 37% |
| Theft of Physical Assets | 37% | 49% | 50% |
| Money Laundering | 4% | 6% | 6% |
| Financial Mismanagement | 22% | 26% | 40% |
| Regulatory/Compliance Breach | 25% | 31% | 36% |
| Internal Financial Fraud/Theft | 19% | 24% | 34% |
| Information Theft/Loss/Attack | 27% | 36% | 36% |
| Vendor/Procurement Fraud | 18% | 23% | 31% |
| IP Theft/Piracy | 16% | 18% | 16% |
| Management Conflict of Interest | 26% | 33% | 41% |

| | Overall Average | Middle East & Africa | North America |
|---------------------------------|-----------------|----------------------|---------------|
| Corruption/Bribery | 20% | 34% | 6% |
| Theft of Physical Assets | 37% | 46% | 28% |
| Money Laundering | 4% | 8% | 3% |
| Financial Mismanagement | 22% | 38% | 16% |
| Regulatory/Compliance Breach | 25% | 23% | 19% |
| Internal Financial Fraud/Theft | 19% | 27% | 10% |
| Information Theft/Loss/Attack | 27% | 29% | 18% |
| Vendor/Procurement Fraud | 18% | 24% | 13% |
| IP Theft/Piracy | 16% | 15% | 18% |
| Management Conflict of Interest | 26% | 43% | 18% |

Hazards in hedging contracts



Most trading on metals markets is well regulated, and most market participants are honest and law-abiding. But the sector has thrown up several scandals over the past few years, with individuals and brokerage houses defrauding employers and clients. Furthermore, metal trading remains one of the few sectors with broker-dealers – companies that act as both proprietary traders and brokers. This creates a vulnerability in the system, which fraudsters can use to their advantage.

Such activities occur most often in futures market trading, not in large-scale options market deals. The main vehicles for these

frauds are cross-trading, front-running, protected trading, and the use of dual accounts.

Cross-trading involves a trader or broker both buying and selling contracts on the same commodity at the same price – in effect selling to himself. Legitimate reasons can exist to do this, for example, when a broker has simultaneous buy and sell orders at a single price from different clients. Often, though, a cross-trading broker is taking a speculative position by trading against another order. This can even mean that a hedger places an order for a company at a price determined by his

own wish to speculate rather than by the client's best interests.

Front-running occurs when a trader with a substantial order to sell, for example, sells a number of contracts to himself before executing the larger order. The latter action may push the market price down, enabling him to buy back his own contracts at a profit. A company executive doing this would need a personal account separate from the one used for the corporate orders. In our experience, such individuals, in order to avoid detection from internal banking control systems, sometimes create accounts with completely different banks or brokers. Front-running is forbidden in the United States and United Kingdom, and any trader or broker found doing it would be banned. It is, however, not always easy to spot, particularly if the irregular trading is done through an account with a different broker.

In protected trading, a trader uses a bona fide hedge order to protect himself from losses on a personal speculative trade by placing the former at a price slightly above the current market level. For example, he might enter an order to sell ten lots at \$5,000 when the market is trading at \$4,990, and then sell on his own account at the lower price. If the market goes down, he can take a profit on the sale, but if it goes up he knows that he can limit his losses by buying the contracts back at \$5,000 by "crossing" – buying and selling the same contracts with the hedge sale.

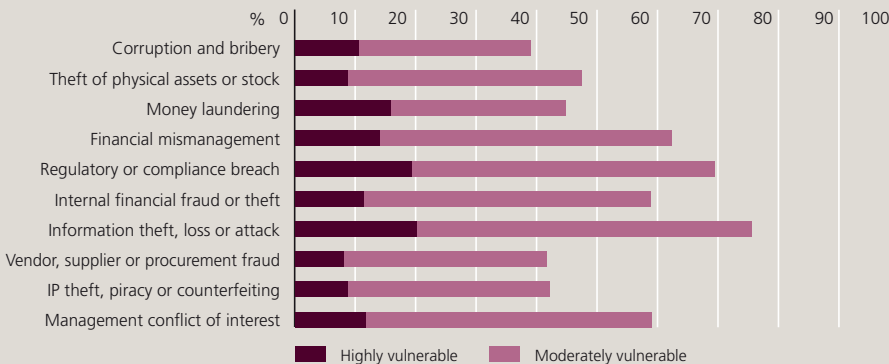
The practice of dual accounts involves controlling two, or possibly more, accounts with the same bank or broker. At the end of trading, when all the day's orders are allocated between the accounts, the trader can put the best trades in his personal account and assign the others to a company one.

Above all, successful hedging fraud requires collusion between the trader and the broker, who both have to work hard to avoid not only internal control systems in their respective organizations but also the scrutiny of the regulators. This is not easy, but once a fraud is established it can be extremely difficult to detect and verify. These considerations mean that metal trading companies need to take regular and proactive steps to counter such frauds. Letting these practices go unchecked can have devastating effects.

REPORT CARD

FINANCIAL SERVICES

- Financial Loss:** Average loss per company over past three years \$12.9 million (157% of average)
- Prevalence:** Companies suffering fraud loss over past three years 79%
- Increase in Exposure:** Companies where exposure to fraud has increased 83%
- High Vulnerability Areas:** Percentage of firms calling themselves highly vulnerable to this type of problem
Information theft, loss or attack (20%) • Regulatory or compliance breach (19%)
- Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud in past three years
Regulatory or compliance breach (35%) • Financial mismanagement (29%) • Theft of physical assets or stock (27%) • Management conflict of interest (25%) • Information theft, loss or attack (24%)
Internal financial fraud or theft (24%)
- Investment Focus:** Percentage of firms investing in these types of prevention in the past three years
Information: IT security (60%) • Financial controls (60%) • Risk officer and risk management system (46%)
Management controls (46%)



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.

CASE STUDY

Benefits of detection



A fraud investigation is about more than finding the perpetrator and recovering the funds. The knowledge that the investigation yields has real long-term value, and can be used to prevent further wrongdoing. Two cases from Hong Kong help illustrate this.

Altered Payee Scheme

Hong Kong listed companies often appoint third party firms as registrars to maintain shareholder registers and handle share-related services, including the distribution of dividends. In one case, a fraudster intercepted a dividend payment issued by such a registrar of around HK\$46 million (US\$5.9 million) and changed the payee's name to his own. He deposited the cheque into a bank account and quickly transferred the funds elsewhere. The fraud went undetected for at least three months until the original shareholder became aware of it.

Kroll's independent investigation found a number of weaknesses which required attention:

- Inadequate fraud prevention measures and controls;
- Lack of a clear allocation of responsibilities and duties among the relevant staff;
- Insufficient written guidelines and procedures;
- Lack of general awareness of possible fraud by staff.

As a result the Hong Kong-listed company suffered a substantial financial loss and sought compensation from the insurer. Kroll's report was able to assist the insurer in determining policy liability allocation.

Mortgage Fraud

In another case, an impostor falsified title deeds and other supporting documents to obtain a mortgage from a local bank. Kroll undertook an independent review of these papers and found a number of discrepancies in the documentation which had gone undetected by the bank's staff. The bank suffered a substantial loss which led to a reassessment of the bank's Know Your Customer policy.

As both of these incidents demonstrate, an important element of any investigation is its application in preventing future frauds.



Susan Lau is a senior director in the Hong Kong office and has over 12 years of banking and accounting experience. She specializes in forensic accounting and fraud investigations involving large, complex, white-collar business crime. Her language skills allow her to focus on the Greater China region.

EIU SURVEY

Fraud remains a very expensive problem for financial services firms, but this sector, unlike most others, held its own against the problem over the last year. Given that the focus of the industry is the use and management of money itself, it comes as no surprise that this, rather than other goods and services, is the main focus of fraudsters.

- The average loss per company of \$12.9 million is down over 10% in absolute terms, and well down in relative terms from last year's survey. The number of companies suffering fraud over the past three years has also dipped very slightly, to 80% from 83%.
- Firms in this industry are more likely than the average for all companies to be hit by financial mismanagement (29% to 22%) but much less likely to suffer from theft of physical assets (37% to 27%).
- Money-laundering remains an important issue: one in eight companies suffered from it in the past three years, a worrying figure given tighter enforcement in this field.

Regulatory compliance is a growing problem and receives too little attention. Compliance breaches continue to plague this highly regulated industry, with 35% of firms – over one-third – affected by at least one within the past three years. Not only is this figure far higher than the survey average (25%), it is also well up from last year's number (29%), so that this is now the most common type of fraud at financial services firms. Concern, however, does not seem to be keeping pace: 19% of companies in the sector now consider themselves highly vulnerable to this sort of fraud, up from 17% last year.

Overall, spending is not keeping up with the growing severity of the problem.

- Although losses from fraud have improved in relative terms, they remain remarkably high. Investment in most anti-fraud measures covered in the survey is slightly more widespread in this sector than in others, but expected new investment is slightly less. Moreover, fewer financial services companies are looking to invest in such tools this year than were last year: for example, only 48% intend to put new money into staff training against 53% last year.
- Perhaps more worrying, the heightened incidence of regulatory breaches is not translating into new spending: only 40% of businesses have compliance controls and training, and just 34% expect to spend new money in this area.

Overall, financial services firms are making some progress against fraud, but companies need to redouble their efforts, especially against regulatory and compliance breaches. The losses involved are much too large to justify complacency.

Written by The Economist Intelligence Unit

New rules cause law firm problems

Governments and regulators in most countries recognize that money laundering is a significant challenge for professional service and law firms. However the regulatory results are different in different jurisdictions and the result can be confusion and complication.

Law firms in the United Kingdom have been accommodating themselves to new anti-money laundering legislation that came into force in December 2007, implementing the European Union's Third Money Laundering Directive. The regulations introduced a risk-based approach, with practitioners expected to assess the level of risk presented by prospective clients and assignments. This permits simplified procedures for low risk activities, but enhanced customer due diligence and on-going monitoring in higher risk areas.

Most law firms in England and Wales have now implemented their procedures, according to a Law Society survey. But it noted that more than half "had difficulty with conducting enhanced due diligence when instructed by clients they had not met. This difficulty was attributed to cultural difficulties with overseas clients, the variability of results from some electronic verification providers and a reluctance of other professionals to be relied upon to certify identity documents."

The EU's rules have been incorporated into national law at an uncertain pace across the Union. The Financial Times reported in July that "More than half of the European Union's

member states - including France and Germany - are being threatened with legal action by Brussels because of their failure to implement anti-money laundering rules designed to clamp down on terrorist financing."

To make matters more complicated, law firms in the US face a different set of regulations. In the EU, there is an obligation on law firms to report suspected money-laundering activity to government authorities. Not so in the US. According to the American Bar Association, "The Association opposes... requiring lawyers to file suspicious-transaction reports on their clients' activities to the extent such a requirement could have an unprecedented impact on client confidentiality, the attorney-client relationship, the independence of the bar, and the compliance-counseling role of lawyers in our society."

This poses some challenges, according to the Law Society:

- Being consistent across multiple international offices
- Representing international clients
- Representing clients with diverse ownership structures.

These issues reflect different legal systems, the roles of law firms and politics. But they also provide potential money launderers with opportunities to exploit differences in procedures between jurisdictions.



Andrew Marshall is a managing director in Business Intelligence & Investigations based in London, having previously held the roles of chief risk officer and head of strategy Europe Middle East and Africa. He spent 15 years as a journalist, including serving as foreign editor and Washington bureau chief for the Independent newspaper.

EIU SURVEY

The sector, including as it does accountants, lawyers, and consultants, should be well informed about the necessity of, and best practice in, implementing anti-fraud strategies: over two-thirds of firms manage fraud prevention, detection, and response internally – about one and a half times the average. This expertise yields results: the sector already suffers relatively little from these sorts of crimes, and the situation is improving.

- The average cost of fraud per firm is the lowest in the survey, just \$1.4 million, or 17% of the overall figure, down significantly from \$2.3 million and 34% respectively.
- The number of companies reporting a fraud in the past three years is also down noticeably, to 74% from 83%.
- Even those who consider their exposure to be growing have decreased – from 89% to 83%.

As might be expected in this industry, information theft remains the biggest concern, and the focus of attention.

- One-quarter of companies consider themselves highly vulnerable to such a threat, and 29% have experienced information theft, loss, or attack in the past three years. Both figures are nearly identical to those of the previous survey.
- IT security remains the biggest focus of new anti-fraud investment in the sector.
- On the other hand, the number of businesses suffering from IP theft, the other big concern for data and knowledge intensive sectors, has seen improvement. Only 13% report recently being the victim of such a fraud, down from 21% the year before.

Complacency is, however, a danger. The sector is doing well relatively, but that still means that three-quarters of companies have been hit by fraud in recent years.

- The use of most anti-fraud strategies covered in our survey is frequently less widespread than average, and fewer companies are investing in them than even last year. Financial controls, for example, are present at only 67% of professional services firms, against 80% among all other companies, and only 47% of the former are spending in this area, against 54% of all other businesses.
- One-quarter of companies have seen internal controls weaken, which is in line with the average, but this sector should know better.
- Although most types of fraud are decreasing, the incidence of management conflict-of-interest rose from 21% to 28%. There is no guarantee that other types of fraud will never do the same. Professional services employees have no special exemption from the sort of temptation which good controls protect against.

Overall, this sector has been very successful in dealing with fraud, but it must not get complacent if it wishes to preserve its record.

Written by The Economist Intelligence Unit

REPORT CARD PROFESSIONAL SERVICES

Financial Loss: Average loss per company over past three years \$1.4 million (17% of average)

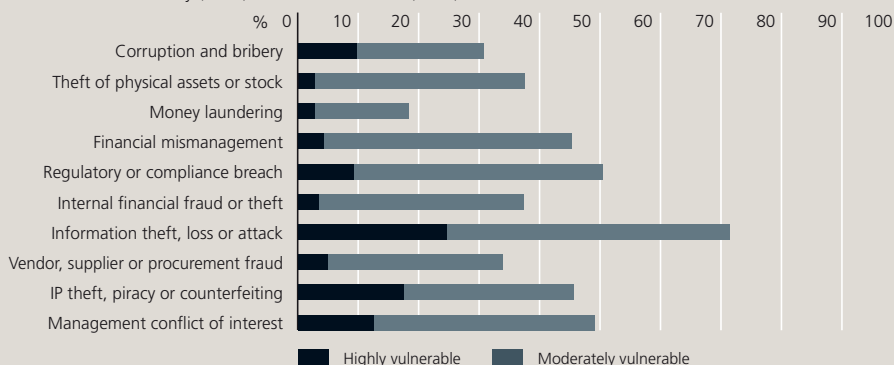
Prevalence: Companies suffering fraud loss over past three years 74%

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

High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable to this type of problem
Information theft, loss or attack (25%) • IP theft, piracy or counterfeiting (18%)

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in past three years
Information theft, loss or attack (29%) • Management conflict of interest (28%)
Theft of physical assets or stock (23%)

Investment Focus: Percentage of firms investing in these types of prevention in the past three years
Information: IT security (58%) • Financial controls (47%)



Protective steps in internal public company investigations



Nancy Goldstein looks at confidentiality and privilege concerns.

An employee lodges a sexual harassment complaint with human resources. An internal auditor uncovers “red flags” of money laundering when reviewing account statements. Compliance receives an anonymous letter alleging improper payments to foreign public officials. These are different scenarios with different actors, but all elicit the same responsibility and concerns for a public company.

In this post-Sarbanes era of greater transparency and accountability, corporations have a heightened duty to conduct internal investigations of potential misconduct. When such allegations arise, companies feel compelled to act with urgency to defuse an often tense situation; however, this is the moment when companies must take the time to assess the potential consequences of conducting an investigation. Corporations must consider that the findings unearthed in investigations may trigger certain disclosure requirements, and arouse the interests of various third parties, most

notably, regulators, shareholders, analysts, and law enforcement. In turn, this interest may result in lawsuits, enforcement actions, and analyst and media coverage.

If a legal protection does not attach to information acquired during an internal investigation, corporations can be compelled to produce such information to opposing parties in litigation, regulators, law enforcement, and other third parties. There are two paramount legal protections for information obtained during an investigation: the attorney-client privilege and the work product doctrine. These protections can apply to all types of information, and the client can assert them in any context from private litigation to government investigation. However, there are specific circumstances in which each such protection attaches, and both require the involvement of counsel.

Situations such as those set forth above which might require an internal investigation do not always come straight to the attention of counsel. Accordingly, the first step toward ensuring that any

applicable protections are preserved during an investigation is to bring counsel (in-house or outside) into the mix to help assess whether an investigation is required and, if so, the potential scope and consequences of such an investigation. Also, counsel can assist the client in deciding when and if it will make assertions of the privilege or work product doctrine. For example, it is important to note that in external investigations, regulators do not take kindly to sweeping assertions of privilege even where applicable, and it is wise to use the privilege judiciously to enhance credibility and to foster a spirit of cooperation.

When a public company decides to conduct an investigation, the first order of business is to coordinate the parties involved internally through counsel, and assess the potential for disclosure, external litigation, and/or litigation. If a company decides to hire an outside investigator, it should consider doing so through counsel to preserve any applicable legal protections. During the course of an investigation, attorneys and investigators must take great care to ensure that both oral and written communications include only parties to the protected relationship. In practice, whether the privilege applies is determined on substance over form, and labeling all communications between attorney and client as privileged will not automatically provide protection; however, it is good practice to label communications which truly are privileged both to earmark such communications for withholding when responding to subpoenas or other requests for information, and to bolster the claim of privilege if called into question.

In addition, attorneys and investigators should segregate their documented analyses and thought processes, so that if investigative findings are disclosed to some degree, any impressions based on such findings can still be preserved as work product. Also, attorneys and investigators should heed the mantra “less is more” by only obtaining information and creating documentation that is crucial to the fact-finding mission to maintain control and limit the universe of information that might be accessible. By taking these basic and other such precautions, all parties involved in the investigation will be sensitive to these confidentiality issues and less likely to inadvertently waive any applicable protections.

Nancy Goldstein is an associate managing director of Business Intelligence & Investigations for Latin America and the Caribbean. She specializes in securities & accounting fraud, FCPA and AML compliance. She spent 17 years as an enforcement attorney for the US Securities & Exchange Commission, NYSE and NASD.

The risks keeping manufacturers awake at night



Manufacturers are faced with a variety of challenges in today's market, including rising energy prices, expensive raw materials, and increasing labor costs. These cost pressures are problematic for even the most savvy and skilled managers, but when the bottom line is affected by unscrupulous procurement staff, they keep those in charge of manufacturing facilities awake at night. There are many ways that fraud can occur in materials purchasing, and it can be guaranteed that any losses by vendors will not be worn by them – they will be passed on in the form of higher prices to the manufacturer.

Asia is the manufacturing hub of the world and procurement fraud is unfortunately a common problem for Kroll's clients. However steps can be taken to reduce the risk of procurement fraud.

In Asia, procurement personnel are, generally speaking, not very well paid, yet they operate independently, are responsible for spending large amounts of money, and are usually responsible for inventory safekeeping. There is an enormous amount of trust placed upon them. The opportunity to make some extra money by illegal means is often too much of a temptation for some who lack integrity. Misconduct commonly committed by procurement staff includes kickbacks, exploiting conflicts of interest, and theft.

Kickbacks. Kickbacks are common in Asia, where for centuries it has been the norm that everyone benefits from a business transaction. An example of a kickback is when the procurement officer receives payment from a vendor in return for the benefit of remaining as a supplier to the manufacturer. Vendors fund kickbacks through price manipulation. The effect is that the manufacturer spends more on raw materials so the vendor is able to fund the kickback.

Manufacturers who use perishable raw materials are particularly susceptible to kickbacks by procurement personnel. In the case where a manufacturer is required to purchase a crop yield, the purchase price should not solely be decided by the procurement department. A similar principle can be applied to manufacturers who sell their by-products or valuable waste material such as gold, silver or copper.

Mitigating the risk of price manipulation to fund kickbacks. Having a price control or a threshold set on the purchase price of perishable raw materials can reduce the opportunity for vendors to offset kickbacks.

The challenge for manufacturers is defining a formula for the purchase price of perishable crops, as the price may be affected by factors such as sales demand, manufacturing

schedules, seasonal availability, crop quality and competitor demand.

Segregation of the decision-making process in relation to the raw material purchase price and sale price for waste product, is one way to mitigate the risk of price manipulation. The purchase price range, and the sale price for waste, should be decided in consultation between several different departments such as sales & marketing, procurement, finance & accounting (including cost accountants), and should require ultimate approval by the general manager. The decision-making process should be properly recorded by the finance department. Any deviation from the agreed purchase price should be properly recorded and receive authorization from the general manager, chief financial officer or other appropriate person.

'Conflicts of interest lead to procurement fraud... usually committed by senior managers'

Conflict of interest. Conflicts of interest lead to another common procurement fraud faced by manufacturers. A conflict of interest in the procurement context arises when a member of staff has a personal interest in a vendor/supplier company. These types of fraud are common in Asia where business transactions are traditionally arranged through family or close friends. Conflict of interest frauds are usually committed by senior managers who have the wherewithal and opportunity. These managers usually have the authority to sign vendor contracts and have the power to direct staff. In Asia it is not common for staff to question the decision of a superior, and it is often the case that staff are aware of the conflict but are not willing to challenge or report it.

Mitigating the risk of conflicts of interest. It is important that staff are aware of company policy regarding personal interests. All employees should receive training and written policy and explanatory material, and should sign a declaration that they have been advised of their obligation to disclose potential conflicts of interest. If the company policy is strict and absolute in regard to the declaration of self-interests, it is recommended that an appropriate clause be included in employee contracts.

Vendor screening also reduces the risk of conflicts of interest among procurement or managerial staff. It makes good business sense to know exactly who the vendors are. This due diligence screening can be undertaken at little or no cost to the manufacturer by making it a contractual obligation of the vendor and making the vendor bear the cost.

Regular review of vendor contracts is another way to lower the likelihood of

REPORT CARD MANUFACTURING

Financial Loss: Average loss per company over past three years \$8.5 million (104% of average)

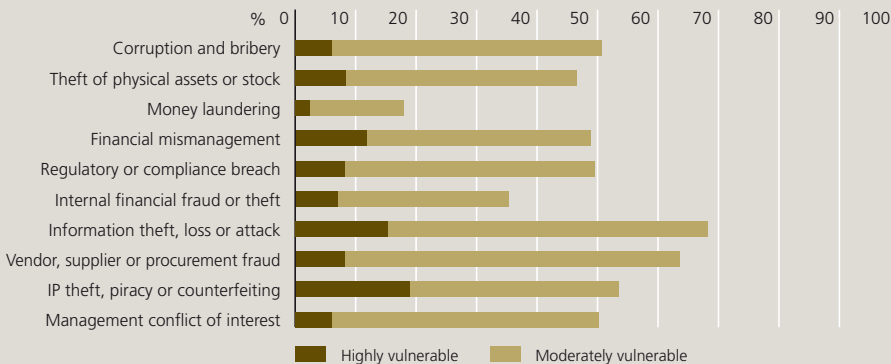
Prevalence: Companies suffering fraud loss over past three years 88%

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

High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable to this type of problem
IP theft, piracy or counterfeiting (19%) Information theft, loss or attack (15%)

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in past three years
Theft of physical assets or stock (53%) • Regulatory or compliance breach (27%) • Vendor, supplier or procurement fraud (25%) • Corruption and bribery (24%) • Information theft, loss or attack (22%)

Investment Focus: Percentage of firms investing in these types of prevention in the past three years
Information: IT security (46%) Physical asset security (44%)



conflicts of interest. It is troubling to consider the number of manufacturing companies in Asia that do not have up to date contracts or whose contracts are not signed by a proper authorized signatory, or whose contracts are unfavorable.

Those above-mentioned risk mitigation strategies are particularly important for companies that have recently acquired an established manufacturing facility, where conflicts of interest could otherwise emerge quickly.

‘Manufacturers have a wealth of material which has become valuable for thieves’

Theft. Stealing is an age-old problem. The variety of methods employed by thieves to perpetrate the crime presents new challenges. Manufacturers have a wealth of material which has become valuable for thieves, including raw material, intellectual property (IP) on new and existing products, IP on manufacturing technology, customer records, office equipment, cash, and the finished products.

Theft of raw material can occur through simply stealing the goods, but suppliers also manipulate systems and receive payment for goods which have not been delivered. Similarly, corruption can lead to inferior materials. Take the example of a perishable goods supplier who is paid according to the weight of his crop: he might be able to manipulate the weight by adding foreign objects such as dirt and rocks to his delivery. Not only is the manufacturer paying more for the crop, foreign objects may damage production equipment and even pose a risk to the consumer.

Mitigating the risk against theft. There are many ways to reduce the chances of theft, including staff rotations, screening all staff, conducting a systems and processes review, and conducting security reviews.

Rotating staff on a regular basis obstructs those who seek to manipulate raw material measuring systems such as the weighing station and quality assurance procedures. Rotation also reduces opportunities for staff to become too close to the raw material suppliers.

Background screening of all staff is essential. The employer-employee relationship is one of trust and therefore it is important that employment history and credentials are checked prior to employment.

A systems and process audit, or healthcheck, is a good way for managers to understand how each process works, and it has the dual advantage of identifying system weaknesses and identifying cost saving measures. Internal reviews are generally undertaken by Internal Audit but they are at times under-resourced and do not include full system and process audits. The system and process reviews can be done in-house by section heads reviewing and reporting on the work processes and weaknesses in another area, broadening the knowledge base of section heads. Often the most effective way to identify systems and process weaknesses is by a combination of internal and external review.

Physical security is an essential component of theft prevention. Often companies do not have the expertise in-house to conduct a security review and Kroll is able to assist with these assessments. An independent review of the physical premises and vulnerabilities in the logistics chain are recommended to reduce losses due to theft. The review may include examination of staff and visitor access, alarm systems, camera placement, secure areas, warehouse security, security guard integrity and a computer system vulnerability check.



Sharon McCarthy is an associate managing director in Hong Kong. She focuses on complex problems such as large scale fraud, compliance issues and financial loss. Before joining Kroll, Sharon was a police officer in the Australian Federal Police (AFP).

EIU SURVEY

For the second year in a row, at an aggregate level, fraud in the manufacturing sector very closely mirrored that of the survey group as a whole. This is no cause for complacency: despite slight reductions in some areas, the incidence of certain categories of fraud remains worryingly high, and the growth in the total money lost should also cause concern.

- The average loss per manufacturer in this year's survey was 104% of the figure for all firms in the survey, up from 101% last year.
- The absolute figures are not comforting: the loss per company was \$8.5 million, up 25% from last year, and nearly nine out of ten companies suffered from a fraud in the past three years.
- Physical theft is the largest problem, and a growing one, having affected over one-half of companies in the past three years, with compliance breaches, procurement fraud, and corruption hurting one-quarter of manufacturers.

Although the actual level of fraud has remained fairly constant in the sector, concern about it seems to be easing.

- In every category of fraud considered in the survey, the proportion of executives who consider their companies highly vulnerable has gone down, except for IP theft and financial mismanagement, which have seen very slight increases. For the two most widespread – physical theft and regulatory breaches – this figure has in both cases gone from 12% to 8%, even though the incidence of both was increasing so that they affected 53% and 27% of firms respectively in the past three years.
- The number of respondents putting new investment into most types of anti-fraud measures has also dropped. For IT security, this has gone from 60% to 46% and for physical asset security from 49% to 44%.

Risk perception has as much to do with people becoming used to a threat present in the environment as with the actual damage that an event might cause. The manufacturing sector is in danger of growing complacent about its fraud problem. Fraud, however, is never predictable. Between the last survey and this one, the average loss per company in the manufacturing sector soared twentyfold. It is far more prudent to bolster the defenses against it than to accept it as a part of doing business.

Written by The Economist Intelligence Unit

Kroll in action

Kroll was engaged by an electronics manufacturer in China who had an expatriate manager in charge of procurement. A whistleblower letter had indicated that the manager was taking kickbacks from vendors in order for the vendors to remain as favored suppliers. A vendor was identified who was fed up with paying kickbacks to the manager, who had apparently been demanding increasing amounts of cash. Kroll became involved and engaged the local police in a sting operation in which the manager was caught red-handed receiving a cash kickback from the vendor.

In addition to liaising with local Chinese officials and law enforcement, Kroll was able to gather electronic evidence, and provide the client with a contingency plan for action after the operation. The contingency plan included notification of the dismissal of the manager to vendors, contacting the wife and embassy of the manager, providing access to counseling and help services for the manager, and assisting the human resources department with follow-up actions.



Preventing data breaches in healthcare

From 2006 through 2007, over 1.5 million names were exposed during data breaches that occurred in U.S. hospitals alone¹. This does not include the other categories of healthcare facilities and services such as home healthcare providers, physician offices, and pharmaceutical companies that also suffered breaches of similar records.

Medical identity theft resulting from patient data breaches is the most difficult to clean up and causes problems beyond financial damage. This crime draws the spotlight because of its perceived magnitude: patients whose data is used for medical fraud (i.e. the perpetrators use stolen information to receive treatment), suffer from insurance eligibility/application issues, as well as potentially life-threatening misdiagnosis due to data on their records that does not apply to them.

While medical ID theft has gained in attention, the risk of being victimized by a Social-Security-stealing fraudster has not decreased. In fact, Kroll sponsored a study earlier this year to find out how hospitals cope in their uniquely precarious position – one open to serving the public, but expected to manage and protect the very private data they use to serve that same public.

Accessibility and vulnerability

Hospitals have an “open door policy,” where doctors, in- and out-patients, students, interns, suppliers and vendors, and visitors come and go greatly at will. Although this

policy is necessary for ease of access and proper care, it also poses a significant risk for identity fraud. This access exposes Personal Identifying Information (PII) and Protected Health Information (PHI) of a vulnerable population including minors, elderly, deceased, newborns, physicians, and the terminally ill.

The healthcare industry also outsources many services, from food preparation, construction, landscaping and maintenance, to collections. This poses a risk as it enables physical access to large volumes of both paper and electronic patient data. In addition, the level of background screening and data security maintained by such third-party organizations is often unknown.

Housing sensitive data

Numerous issues keep the security of patient information at the forefront for healthcare organizations. Patient data collected and stored in hospitals and healthcare facilities is possibly the most valuable and content-rich data for fraudulent use and profitability. In addition to name, Social Security number and date of birth (the golden combination), records in these facilities also contain mailing addresses, insurance policy information, medical history, and, in some cases, credit card and financial information to expedite billing and payment – more data in one record than those of any other source such as banks, schools or HR departments.

This wealth of information is a treasure trove to identity thieves, who can gain access to large numbers of data elements in one setting and can use them repeatedly over long periods of time.

The Study

In Spring of 2008, Kroll, leader in data security, privacy and data breach response, selected HIMSS Analytics² to lend its industry expertise to study how healthcare organizations in the United States are dealing with the priority requirement to secure patient data in the current environment.

Kroll had long suspected that the vulnerability of healthcare organizations was particularly great – and for the most part, unexamined. In the roster of client organizations that had chosen Kroll to provide data breach incident management, over 20% represented the healthcare industry. Kroll had seen the weaknesses up close:

- In a culture of caring, staff may break protocol and unintentionally sacrifice data safety to protect patient records in a way they personally believe works better.
- Facilities that are compliant with the Health Insurance Portability and Accountability Act (HIPAA) may consider such adherence to mean that all important data is tightly protected.

The broad objective of this research was to identify how aware respondents were of the laws in place regarding patient information, the measures and tools that hospitals were taking to secure patient information, as well as to identify how they were dealing with security breaches which may have already taken place.

To investigate, HIMSS Analytics surveyed 263 U.S. healthcare industry professionals in January 2008. Research participants included IT professionals (50%), Health Information Management (HIM) managers (21%) and chief security officers (12%), among others working in the area of information management.

Kroll's expectations were confirmed. The study revealed a lack of awareness around the frequency and seriousness of identity theft, which in turn negatively affects efforts to contain the problem and reduce the risk. There are a number of factors contributing to this phenomenon, including regulatory shortcomings.

Regulatory shortcomings

Nothing in HIPAA requires organizations to report a patient data breach. However, the issue of notification has risen to the state level; as of July 2008, 44 states have a breach notification law. As a result, healthcare organizations must not only be compliant with HIPAA, but also be compliant with their own state laws. Still,

REPORT CARD HEALTHCARE, PHARMACEUTICALS AND BIOTECHNOLOGY

Financial Loss: Average loss per company over past three years \$7.8 million (94% of average)

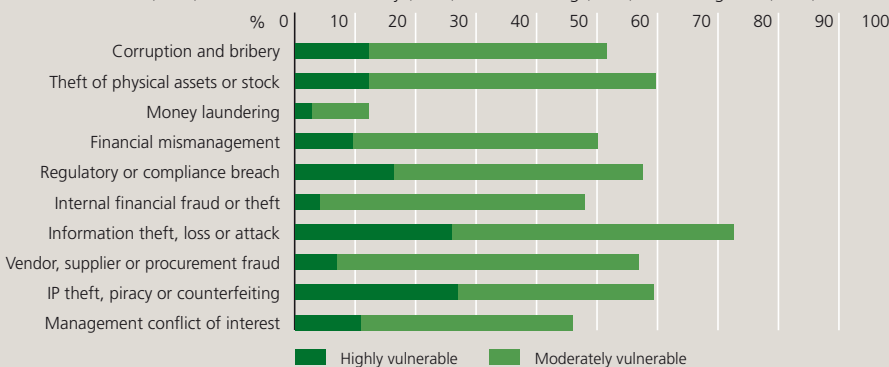
Prevalence: Companies suffering fraud loss over past three years 86%

Increase in Exposure: Companies where exposure to fraud has increased 89%

High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable to this type of problem
IP theft, piracy or counterfeiting (27%) Information theft, loss or attack (26%)

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in past three years
Theft of physical assets or stock (41%) • Regulatory or compliance breach (37%) • Management conflict of interest (28%) • Information theft, loss or attack (26%) Financial mismanagement (26%)
Internal financial fraud or theft (24%) • Vendor, supplier or procurement fraud (24%)
IP theft, piracy or counterfeiting (22%) • Corruption and bribery (20%)

Investment Focus: Percentage of firms investing in these types of prevention in the past three years
Financial controls (60%) • Information: IT security (57%) • Staff training (46%) • Due diligence (46%)



these regulations lack a clear roadmap for follow-up action and for notifying affected individuals in the event of a breach.

Since there is no overarching federal law, states have created and instituted laws based on independent discretion. Therefore, the laws are particularly diverse, ranging from very specific to relatively general requirements. Notification laws are based on “triggers,” or what initiates the need to notify at all. As a result, state laws vary considerably regarding who should be notified. Some states require that the entity notify consumers, state agencies, and/or credit reporting agencies. For others, the requirement to notify is predicated upon the number of individuals affected by the breach.

It should also be noted that some state notification laws may only apply to breaches by corporations and/or other private entities, or to state agencies, but not to both.

Considering the variety of breach definitions, the diversity of discretionary requirements, and the lack of distinct direction from HIPAA, it is not surprising that only 56% of surveyed facilities that had experienced a data breach actually notified the patients of PHI and PII losses.

Compliance versus risk

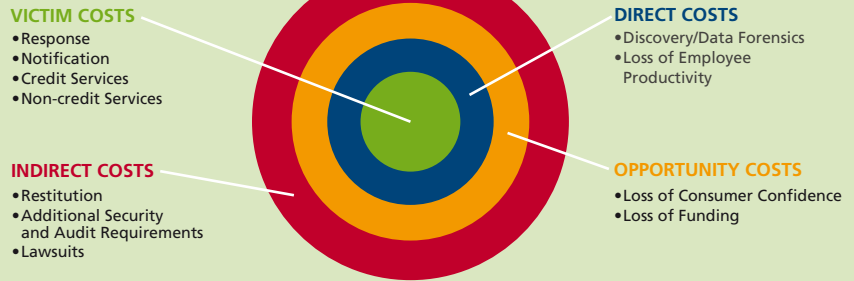
Awareness of and compliance with policy requirements does not mean a facility is providing holistic protection of patient data. On average, respondents ranked their familiarity level with the HIPAA at 6.53 (on a scale of 1-7, with seven being the highest) and nearly 75% claimed a familiarity level of seven. The high level of HIPAA familiarity stems from the commencement of audits and the resulting penalties for non-compliant facilities.

A singular focus on regulatory compliance can lead organizations to have a “checklist” approach to security, merely checking off regulatory compliance implementation items to the exclusion of a thorough analysis of the threats. Adherence to regulations is more of a “compliance-driven” approach than it is a “risk-based” methodology. Unfortunately, this perspective often leaves blind spots prone to exposure.

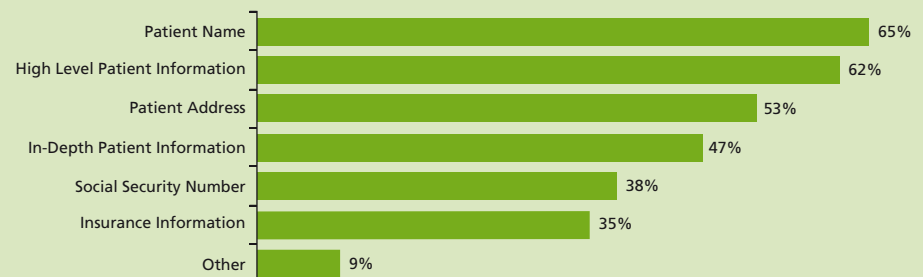
Lack of awareness of the impact of a data breach

Survey results revealed a notable lack of awareness around the cost and impact of a data breach. In the study sample, only 18% of organizations that had experienced a breach believed there was a negative financial impact. Yet, in the past two years, the cost of a data breach to organizations rose an estimated 43% with an average cost of \$197 per compromised record.³ Additional costs include discovery, response and notification, lost trust of patients and employees, lost employee productivity, additional regulatory fines, damage to reputation, opportunity costs, and other indirect costs.

True cost of a data breach



Data Compromised in a Security Breach



Recommendations

Healthcare organizations commonly take a reactive approach towards security enforcement and breach planning. However, this Kroll report demonstrates that in order to safeguard patient data while still maintaining the highest quality of care, healthcare organizations must broaden their risk management measures to:

- Minimize data hoarding – Discourage downloading, storing multiples – since medical facilities are bound to store data beyond discharge and even beyond death, do what you can to prevent it being copied, saved, shared and stored independently. If each department has its own copy of a record, it is that many more times vulnerable to inappropriate access.
- Maximize access management – Information should be available on a need to know basis. Access to PII should be limited to those who must have it to do their jobs. Consider a unique, hospital-assigned identifier if it is necessary – but there is no reason why a laboratory clerk or radiology technician should have a patient’s Social Security number.
- Change with change – It is common for a medical facility to give a third party vendor access to its data for projects. Remove or cancel that access when the project is over. Be sure the vendor lets you know if their people on the project change.
- Optimize employee education – Encourage staff and vendors to treat SSN and DOB like protected health information. Capitalize on the existing sensitivity to privacy and HIPAA requirements; build on that “habit” and

familiarity of actions so that employees treat all patient data as reverently

- Recognize scalability – An organization’s policies and procedures of data security must be scalable to its size. This report found that a data breach is three times more likely to happen at a larger facility (more than 100 beds) than a smaller facility (under 100 beds).

Organizations must continue to be vigilant about ensuring that their security policies and procedures are enforced, and that educating employees remains a top priority.

Progress towards better security and safer patient data environments will start with a paradigm shift in the approach to patient data security, treating it as an ongoing operational and behavioral change that guards against both theft of patient data records for fraudulent purposes as well as inappropriate access during treatment and beyond.

1 www.attrition.org, 03/01/2008

2 HIMSS Analytics collects and analyzes healthcare organization data relating to IT processes and environments, products, IS department composition and costs, IS department management metrics, healthcare delivery trends and purchasing related decisions. HIMSS Analytics is a wholly-owned, not-for-profit subsidiary of the Healthcare Information and Management Systems Society (HIMSS).

3 Ponemon Institute, 2007 Annual Study: U.S Cost of a Data Breach, 11/2007, p.8



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



Strengthening information security

A fraud prevention measure in the pharmaceutical industry

It is often said that knowledge is power, and in many cases knowledge is not only power but also income and profits. Pharmaceutical companies invest billions in research and development of medicines, formulations, and compounds – research that often turns out to be seriously compromised due to the lack of an effective information protection system providing a reasonably secure environment.

Security audits commonly identify highly confidential documents left abandoned on

printers or fax machines, or unshredded sensitive documents discarded in wastepaper baskets. And removable storage devices with large amounts of company data passed from one PC to another often end up on hard drives of employees' PCs when working at home.

The legal protection of trademarks, patents, and registered copyrights are fundamental issues for research and development companies; however, industrial and intellectual property must also be

safeguarded by tools and procedures that prevent information from leaving the company environment and falling into the hands of competitors. While legal safeguards do exist, if an information leak takes place, the damage is usually already done and legal remedies can take years.

Aware of these risks, and as a result of their own experiences, large corporations have begun to protect themselves. Companies are implementing protection systems and raising employees' awareness of the issue

by means of seminars and courses on the various data gathering and competitive intelligence techniques used by competitors.

Protection of information in the pharmaceutical industry is essential, not only to ensure that competitors do not develop the same product within a shorter time span and at the expense of another company, but also to avoid the development of medicines, generic or under a different name, that use part of the formula with a similar composition but different proportions, which have not been submitted to the same controls as the original ones. In this case, the prestige of the laboratory that develops the original medicine is seriously harmed, as consumers might confuse the inferior product with the more popular one.

Sensitive information flows through several channels within organizations: printed documents, oral communications, and electronic messages, among others. All channels must operate within an effective information protection system that guarantees a reasonable level of security and prevents the removal of the company's confidential data.

Where to start?

Before implementing a protection system, it is important to categorize information assets – perhaps as critical, confidential, or extremely sensitive – as well as logging their location and the media in which they are stored.

Once this classification is completed, choices need to be made in terms of the protection system, suitable segregation of information and lines of responsibility so that those who handle the information are responsible for its safekeeping and accountable in the event of a leak.

In the pharmaceutical industry, the specific characteristics of information must be specially preserved since such data is the basis for research that requires a high level of accuracy and veracity, as well as the necessary confidentiality to protect the company's R&D investment.

Safeguarding the confidentiality of information protects the company's investment in R&D against both competitors and disloyal or disgruntled employees who are seeking personal gain through the sale of industrial secrets.

The integrity of information is also fundamental in the research and development process which demands that the information used is reliable and accurate. It is also essential that this information be properly backed up in the event of data destruction which would result in the loss of the investment as well as years of research.

The characteristics of the information are also preserved by physical security systems and security procedures that prevent theft of physical assets derived from information obtained through research, such as test tubes containing substances used in the development process for future medicines.

Once the parameters of information safeguarding and availability have been set, users should have due responsibility for these assets so that they ensure the security of the working environment and are liable for their actions or possible negligence.

What happens if there is an information leak? Often nobody knows anything about it and it is difficult to identify the person responsible for the leak since companies don't always have defined responsibilities regarding their information assets. In addition, the information has generally circulated through so many different places, that it is almost impossible to determine where the fault lies or if there has been negligence at any stage.

Human vulnerabilities

The information user is an indispensable link within the protection system, so much so that, even if a security system is in place, the system will not fulfill its protective mission if the user is not aware of the risks involved and is not using the information in a responsible manner.

Examples of such situations include indiscretions committed in a social environment, the use of weak passwords in computer networks, or the indiscriminate use of the phone in any place and situation.

Users must be aware of the risks and especially of the techniques used by third parties for obtaining confidential information, as well as being made aware of the protection tools they have at their disposal.

Therefore, the protection of information should not be seen only as an expense rather it is a way of ensuring the profitability of multimillion dollar R&D investments. It is also a way of sharing information at the proper time and place and guaranteeing that data is reliable, accurate and in a secure environment. Spending thousands of Euros in identifying vulnerabilities and correcting them can protect an investment of tens or hundreds of millions, which once compromised is difficult to recover.



Javier Cortés is director of Security and Crisis Management Consulting Services in Madrid. Prior to joining Kroll he was director of security at Plus Quam in Central America. He has experience in crisis management, security engineering, fraud control and information security audits such as NATO security audits.

EIU SURVEY

Although the last year saw a welcome reduction in the financial loss from fraud in the healthcare, pharmaceuticals, and biotechnology sector, this masks underlying trends pointing to an increase in the range and diversity of fraudulent activity.

- The average loss per company is now \$7.8 million, about average for all industries, but well down from last year's \$11.7 million.
- Of the categories of fraud considered in this research, only one – money laundering – decreased in frequency. Another – IP theft – stayed roughly the same. The incidence of the other eight categories all increased, sometimes substantially: the proportion of companies reporting physical theft went from 25% to 41%, and that for corruption jumped from 8% to 20%.
- This sector shows the widest range of problem fraud areas, with every type of fraud in the survey, bar money-laundering, affecting at least one in five companies.

The health sector is maintaining its focus on information and IP related fraud, which makes sense in a knowledge-based industry, but does not seem to be recognizing the growth of problems in other areas.

- Just over one-quarter of companies consider themselves highly vulnerable to IP theft and information loss, slightly up from last year. IT security accordingly remains one of the areas where most companies will be spending further, and nearly one-half of firms already have IP monitoring in place, well above the survey average of 35%.
- IP abuse, however, was one of the less frequent frauds in the sector, and one of the few not to grow. Concern over problems such as corruption and compliance breaches has dropped, even as they became ever more common. The latter affects more than one-third of companies, but only 17% consider themselves highly vulnerable to it.

The healthcare, pharmaceuticals, and biotechnology sector faces a growing fraud problem, the full extent of which it needs to recognize. The progress in reducing economic losses could easily reverse should the many, relatively smaller crimes from which it is suffering expand in size.

Written by The Economist Intelligence Unit

The changing face of online brand abuse

Whether you work at a large company centered on a mega-brand, a company with a portfolio of world-class brands or an emerging start-up, the brand breathes life into every aspect of the business, guides every customer interaction and drives market perception. The flip side of the “brand coin” are the online thieves and brandjackers who earn a living by attacking leading brands. These attacks come from multiple directions, often simultaneously and always at warp speed.

Constant growth and changing targets

MarkMonitor’s most recent Brandjacking Index™ quantified these attacks by examining 30 leading Interbrand-ranked global brands through 2007 and the first quarter of 2008. It found the biggest growth in brandjacking abuse was in mainstream product categories. Automotive brands rose the most sharply as targets for brandjacking with a 99% increase and food and beverage products with a 77% increase. Cybersquatting continues to be the most common method of brandjacking observed with more than 400,000 exploits in the first quarter of 2008 alone. This represents a 40% increase for the year beginning 2007.

The recent news on phishing continues to be worrisome. Phishers are carefully picking the most desirable targets. During the last quarter of 2007, there was profound growth in the number of new organizations targeted by phishers, with 122 companies observed for the first time as the subjects of an attack. This is the biggest increase in

any quarter of the year, showing that the phishers are widening their focus. MarkMonitor also saw seasonal shifts in the types of target industries, and continued increasing sophistication in the types of exploits used by phishers to obtain individual user account information.

Overall, 412 different organizations were targets of phishing attacks last year, which represents an increase of 37% over the number observed in 2006. November was a record month for phishing targets, with 275 targeted organizations.

Vigilant brandholders do have an effect

MarkMonitor has seen a decline in some areas of brandjacking, in domain kiting and Pay-per-click attacks, which is believed to be as a result of brandholder vigilance. But as long as there is money to be made, you can be sure to see brandjackers evolve their techniques – and seek fresh brand targets – to line their pockets.

For the full story on our most recent Brandjacking Index, please visit www.markmonitor.com to download a complimentary copy.

MarkMonitor is in the business of protecting enterprise brands online, helping strong corporate reputations become even stronger in the digital world. We 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

EIU SURVEY

The fraud situation in the technology, media, and telecom sector is more positive than in most other sectors. As knowledge industries, their most pressing issues are information and IP theft, both of which are getting increased attention.

The overall level of fraud is lower than the survey average and has seen little increase from last year, although the nature of the fraud has been shifting.

- The average loss per firm is \$5.6 million, more than last year’s \$4.9 million, but this growth is at about one-half the rate of the overall average.
- The percentage of companies affected by fraud, 79%, is also up slightly, but is still one of the lowest in the survey.
- The nature of the fraud has been shifting with certain categories becoming more common – 33% reported experiencing physical theft and information theft in the previous three years, against 28% and 27% in the last survey – while others have dropped – only 14% reported procurement fraud and corruption, against 24% and 21% in 2007.

Accompanying the rise in information theft has been a very rapid rise in the number of companies aware of the risks which a knowledge-based sector faces.

- The number of companies which consider themselves highly vulnerable to information loss, theft, or attack has almost doubled, from 21% to 41% in the last year, and the figures for vulnerability to IP theft also show a large increase, from 22% to 34%.
- The proportion of firms spending on IT protection and IP monitoring has accordingly also gone up – to 64% and 54% respectively. The latter figure is more than one and half times the survey average.
- While focusing on the most worrying areas, the industry is also paying more widespread attention to protection of physical assets, as physical theft remains one of the most common frauds its companies see.

The technology, media, and telecom sector does not yet have a major problem with fraud, and many companies are taking sensible steps to address the most pressing threats. They simply cannot afford the impact of extensive information and IP theft.

Written by The Economist Intelligence Unit

REPORT CARD TECHNOLOGY, MEDIA AND TELECOMS

Financial Loss: Average loss per company over past three years \$5.6 million (67% of average)

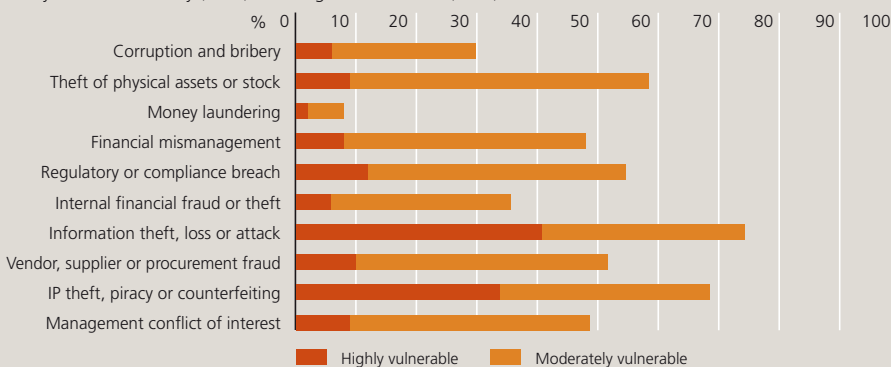
Prevalence: Companies suffering fraud loss over past three years 79%

Increase in Exposure: Companies where exposure to fraud has increased 90%

High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable to this type of problem
Information theft, loss or attack (41%) • IP theft, piracy or counterfeiting (34%)

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in past three years
Theft of physical assets or stock (33%) • Information theft, loss or attack (33%) • IP theft, piracy or counterfeiting (22%) • Management conflict of interest (21%) • Regulatory or compliance breach (20%)

Investment Focus: Percentage of firms investing in these types of prevention in the past three years
Information: IT security (64%) • IP and trademark monitoring program (54%) • Financial controls (49%)
• Physical asset security (47%) • Management controls (47%)



Guidelines for expanding in developing countries

As world demand for metals, minerals, timber, and petroleum grows, natural resource companies are constantly looking for new sites with raw materials to explore and develop. Most often, these sites are in remote parts of developing countries, with limited access to infrastructure including water, electricity, housing, or skilled labor.

Once a property is acquired, the rush begins to bring operations online as quickly as possible. To do so effectively, local managers must be adept at finding suppliers for staffing, equipment, and support services. These managers often require flexibility from the company to make things happen. While this is understandable, the potential implications for internal fraud are great. According to the survey for this edition of the *Global Fraud Report*, nearly four in ten natural resource companies suffered from management conflict of interest in the last three years.

In Kroll's experience, two patterns of internal fraud repeat themselves in this sector, each illustrated in the following cases.

All roads lead to the same supplier

One mining company began using a firm to provide local assistance for cleaning and maintenance services. Within a year, the same firm was sourcing temporary labor for the mine, as well as providing transport services for employees. After an audit raised concerns about the mining company's degree of dependency upon this sole provider, it began using other suppliers, but all had the same address. A closer review revealed that the mine's local general manager held shares – through a cousin – in these businesses.

Emergency orders are the norm, not the exception

A petroleum services firm had developed a relationship with a company to manage its inventory of spare parts. An anonymous report to the former's integrity/whistleblower hotline tipped off corporate management to irregularities in this link. Data mining of purchases during the previous year revealed that "emergency" orders for non-essential equipment and spare parts for production machinery represented over 50% of the purchases made from the supplier. Given that the supplier was also contracted to provide inventory management, it was alarming to see how little planning was evident. Further investigation showed that because orders were registered as urgent, the supplier was able to charge a 20% premium over preapproved prices. It was subsequently revealed that the purchasing manager was receiving kickbacks for classifying orders, including those for common light bulbs, as emergencies.

The combination of the aggressive search for raw materials, the need for extensive local managerial autonomy, and limited supply options can, if left unmonitored, easily enable costly frauds to occur.



David Robillard is head of the Mexico office for Kroll. He has more than 15 years of experience in the fields of business intelligence & investigations, working with global clients in multiple industries. He is a winner of the International Award of Excellence for People and Process from SCIP (Society for Competitor Intelligence Professionals).

EIU SURVEY

For the natural resources sector, fraud is a very serious and rapidly growing problem.

- The average loss per company from fraud rose markedly from \$11.5 million in the last survey to \$18.1 million in the most recent, the biggest for any sector. The industry could expect a slightly elevated number here because its companies are larger on average. Nevertheless, the growth in these losses is far outpacing that in other industries.
- About 70% of the growth in the total amount of fraud comes from the rapid increase in the number of companies affected: in the last survey only two-thirds reported being hit in recent years; now 92% do.
- Various categories of fraud have also seen a marked increase in activity: according to the most recent figures, 26% of companies have seen financial mismanagement in the past three years, nearly double the previous level of 14%; 29% had also suffered from information theft, up from 15%; and 17% had lost out to IP theft, up from just 5%.

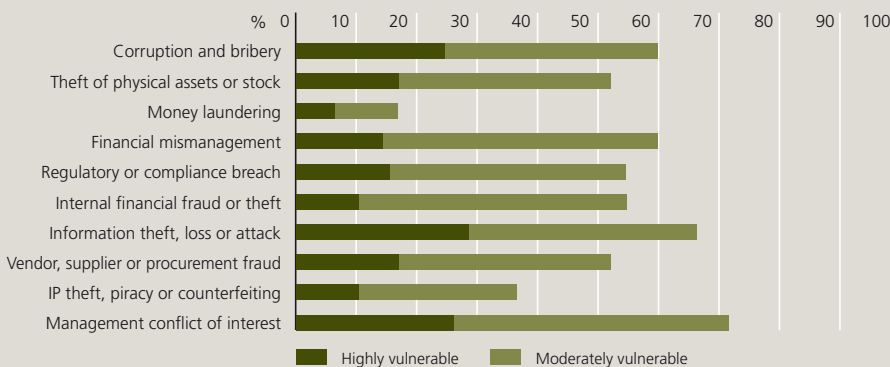
The effects of this growth on perceptions of exposure and vulnerability have been uneven, probably because the natural resources industry has a reputation for relatively high levels of attempted fraud already. This arises in part from its need to obtain raw materials wherever they are available, no matter how ill-suited the business environment. Again this year, entry into new, riskier markets was the sector's leading cause for increased exposure to fraud, cited by over one in three companies. This background explains why the proportion of companies reporting a greater exposure for whatever reason has risen to 78%, but is still far below the survey average of 84%. On the other hand, those feeling highly vulnerable to specific issues have seen uneven change. Perceptions around areas long known as problematic, such as corruption, saw little change. Types of fraud which were previously less of a concern, such as information theft – where the proportion of highly vulnerable firms grew from 19% to 29% – are now more firmly on the radar.

As a sector used to dealing with fraud, natural resources companies typically deploy more anti-fraud measures than the average, and are also undertaking more widespread investment in them: for example 65% of sector companies are spending on financial controls against 54% of all businesses, even though more of the former already have such controls in place (87% to 80%). Although addressing the issue seriously, firms in this industry must take care not to overlook old risks while attempting to protect themselves against newly recognized ones.

Written by The Economist Intelligence Unit

REPORT CARD NATURAL RESOURCES

- Financial Loss:** Average loss per company over past three years \$18.1 million (220% of average)
- Prevalence:** Companies suffering fraud loss over past three years 92%
- Increase in Exposure:** Companies where exposure to fraud has increased 78%
- High Vulnerability Areas:** Percentage of firms calling themselves highly vulnerable to this type of problem: Information theft, loss or attack (29%) • Management conflict of interest (26%) • Corruption and bribery (25%)
- Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud in past three years: Theft of physical assets or stock (39%) • Management conflict of interest (39%)
- Information theft, loss or attack (29%) • Financial mismanagement (26%) • Corruption and bribery (26%)
- Internal financial fraud or theft (25%) • Regulatory or compliance breach (20%)
- Investment Focus:** Percentage of firms investing in these types of prevention in the past three years: Financial controls (65%) • Management controls (55%) • Information: IT security (53%) • Physical asset security (48%)





Compliance: It's just good business sense



Blake Coppotelli tackles one of the most complex issues facing business: The impact of compliance on global corporates.

Enron, Tyco International, Global Crossing, Parmalat, Peregrine Systems, and World Com changed the compliance world. The infamous fraud scandals surrounding these companies were responsible for the enactment of the Sarbanes-Oxley Act and played an important role in the evolution of the renewed enforcement of other regulations such as the Foreign Corrupt Practices Act ("FCPA"). Sarbanes-Oxley and the FCPA, along with the Patriot Act and US anti-money laundering statutes, now place significant requirements on foreign companies to institute compliance measures in order to operate in the US and reduce their exposure to prosecution by the Security Exchange Commission ("SEC") and/or the Department of Justice ("DOJ").

The FCPA, for instance, applies to any domestic company, its foreign subsidiary, and any non-US company whose securities are listed in the United States, and prohibits any person acting on behalf of such company from making a payment to a foreign government official for the purpose of obtaining or retaining business. The practical effect of the FCPA is to place significant compliance requirements on those companies, foreign or domestically owned. These requirements include, but are

not limited to, conducting due diligence on business partners and third parties acting on their behalf, developing a written compliance and internal control program, training thereon, and a process that proactively tries to prevent and deter FCPA violations from occurring, including audits of the program to ensure its effectiveness.

The significance of the FCPA cannot be understated. Forbes magazine reported last year that the DOJ investigated more cases of foreign bribery in the last five years than it did in the previous twenty. This significant increase in enforcement actions continued through 2007 with a record \$44 million in fines and penalties imposed against Baker Hughes, Inc., and \$26 million fines imposed on three UK based subsidiaries of Vetco International Ltd. In July 2007, Gibson, Dunn & Crutcher LLP reported that it found from public filings, corporate disclosures, and contacts that approximately 100 foreign and domestic companies have been notified by the federal government that they are currently under investigation for FCPA violations. The staggering volume of FCPA investigations, and the record fines and penalties being imposed by the DOJ, has significantly increased the attention foreign companies are paying to compliance.

Sarbanes-Oxley, particularly Section 404, mandates similar compliance requirements on foreign companies. The act applies to any non-US companies that have securities listed on a US stock exchange or are quoted on NASDAQ, and mandates that such companies report annually to the SEC on the effectiveness of their internal controls over their financial reporting. Approximately 425 non-US companies are listed on the New York Stock Exchange ("NYSE"). As of January 2007, the NYSE reports that these non-US companies have a capitalization of about \$9.6 trillion or about 38% of the total capitalization on the exchange. Around forty of these companies are UK based including some of the worlds largest, e.g., BP, Barclays, HSBC, and British Telecom. German based BASF estimates that it spends \$30 to \$40 million per year on Sarbanes-Oxley compliance. The estimate for large UK based companies is from £10 to £20 million (GBP) for first year compliance alone.

If the financial and logistical weight of these US regulations weren't enough, the U.S. Federal Sentencing Guidelines (Chapter 8) places compliance mandates on any foreign company that is within the jurisdiction of any US law. Interpreting the guidelines, the recently issued DOJ

“McNulty Memorandum” provides federal and, indirectly, state prosecutors with a road map to determine the proper treatment of an organization when it, or any representative thereof, is suspected of violating any US law. The memo and guidelines place severe consequences on an organization if it does not have, at a minimum, policies, standards and procedures defining the compliance roles and responsibilities of senior management and the board of directors. Other requirements include a clear and effective mechanism for reporting fraudulent activity, established guidelines on how to respond to potential internal fraud and appropriate disciplinary procedures, and a definition of the company’s relationship with external auditors and counsel. In addition, the guidelines require continuous monitoring and testing of the compliance program.

Is the US over-regulated? That has been a common view in the media and amongst some business commentators. The claim has often been made that New York City has lost ground to London as the world’s global financial center, and that US regulations were the primary cause for New York City’s divergence. UK and European based companies have increasingly decided to list their shares in London, as opposed to New York City, because of the perceived harsh requirements of the above-described US regulations. There is also an unresolved issue that compliance with Sarbanes-Oxley, specifically information required to be disclosed in item 8.1 of the Act’s registration form, may violate the UK’s Data Protection Act of 1998. NYSE data regarding active listings on the exchange since 2004 shows a steady decline in the number of listings of UK companies. This concern about US market competitiveness spurred Treasury Secretary Henry Paulson to convene a special conference on the issue in March 2007, and to remark that the right balance must be struck between protecting investors and promoting competition. In terms of the rivalry between New York and London, that led many to wonder if the balance between the two centers was out of kilter.

It is worth pointing out that the UK has regulation of its own, and domestic and international companies are subject to potentially similar regulations. The Money Laundering Regulation 2007 is the UK’s implementation of the Third EU Money Laundering Directive, which establishes requirements on companies to prevent money laundering and terrorist financing. The UK Anti-Terrorism, Crime & Security Act 2001 strengthens the UK laws on bribery and corruption and gives UK courts jurisdiction over bribery committed anywhere by UK domiciled companies

and their employees. Corporate governance in the UK is moving towards similar regulations. The Basel II and Solvency II agreements have similar levels of compliance to Sarbanes-Oxley.

In addition, twenty-nine members of the Organization for Economic Cooperation & Development (“OECD”) and five non-member countries signed a mandate to combat bribery of foreign public officials in international business transactions. The mandate lists sanctions that are severe and include forfeiture, judicial supervision, confiscation, and business interruption.

But in view of everything that has happened in the last year to the financial services sector in particular, is it also the case that the UK is under-regulated? Its light-touch, risk-based approach has confronted severe challenges, and not always with success, as the UK’s Financial Services Authority has recognized. Nor is the UK’s record on corruption and its prosecution exactly spotless.

It is also important to remember there are reasons why the US has instituted these regulations. Resolution of these regulatory compliance issues for non-US companies may be long in coming. We cannot forget that the heart and purpose of compliance is to prevent fraud. This is a very simple concept that inherently makes good business sense, regardless of the level of regulatory requirements. From a purely business context, instituting effective procedures to deter, prevent, and identify fraudulent activity lowers a company’s business risks, maximizes its public persona, and adds to shareholder and consumer value and confidence.

The result of regulation and the changing business environment is that companies in Europe and the US increasingly understand the purely business benefits of instituting anti-fraud processes. They are conducting risk assessments to determine their fraud weaknesses. Those companies that do not have the internal resources to adequately perform a self-assessment are hiring third-party consultants to conduct the audit and to create and implement effective remedial actions. US and UK companies are beginning to request best practices in looking at the adequacy of their integrity policies and procedures, accounting controls, hiring processes and pre-employment screening protocol, management and employee training, third-party/vendor screening procedures, and financial and investigative due diligence activities.

By far the biggest focus for US and UK based companies is in the field of due diligence. This has now become a staple for companies seeking to significantly decrease their transactional fraud risk. Best practices

in both the US and the UK have evolved to require a thorough investigation into the background of all new officers, directors, and key management personnel of the organization, all potential business partners and their representatives, including officers, directors, and key management, material customers, vendors, consultants, and agents, and parties involved in material financial transactions (e.g., IPOs, mergers and acquisitions, and financing). The objective now is to assess the financial background, reputation, integrity and bona fides of all parties to a business transaction, including the principals, directors, and/or officers of any entity seeking to do business with the company. It isn’t sufficient any more to fail to ask the questions.

Risk is also seen on a broader spectrum than purely financial or criminal issues. Companies are increasingly trying to identify risks related to a potential business partner’s ethical track record, regulatory compliance, market condition, hidden interests, conflicts of interest, environmental liabilities, and any non-disclosure or misrepresentation of material facts. Information sought to be identified includes facts related to a potential business partner’s corporate structure and ownership, historic and current profile of business activities and reputation, significant financial data, bankruptcy history, credit risk, history of litigation, regulatory compliance, frequency and significance of administrative proceedings, media profile and reports, bank referencing, including verification of the potential partner’s standing and status with their banks, and professional/trade referencing and track-record.

Those companies that are instituting these best practices are significantly minimizing their fraud risk, while in most instances also effectively adhering to US compliance mandates. This secondary benefit goes a long way to protecting them from financial and reputational damage, and criminal and civil liability resulting from any unknowing regulatory breaches. So, while the compliance world waits for some type of relief or direction, US and UK companies are taking the bull by the horns, and are practicing good business sense by instituting anti-fraud measures that satisfy many of their compliance requirements. Whatever the difference between their regulators, the businesses themselves know it makes sense.

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

Profile – Leading express and mail provider shows the way

Ten years ago, it would have been unthinkable for a top manager of a major international organization to openly include the fight against corruption in his agenda. Today, things are different. It is now widely presumed that corruption hampers economic growth, discourages public and private investment, and increases poverty. The former president of the World Bank James Wolfenson exhorted the international community to “deal with the cancer of corruption, because it is a major barrier to sustainable and equitable development”. TNT is a leading global express and mail business that has also taken the lead within the field of preventing fraud and corruption. Having signed the UN’s Global Compact, it included the 10th principle on anti-corruption in its business principles. However, TNT has taken this work further than many other companies.

TNT has invested heavily in its security frameworks globally, demonstrating a worldwide investment in security provisions, practices and procedures. Its “Integrity Program” forms part of this emphasis towards matters other than just the physical security aspects within a multinational organization. For the benefit of its stakeholders, TNT does everything it can to improve its integrity.

TNT is aiming towards ethical transparency and takes this aspect extremely seriously. Responsible for the company’s core Global

Investigation Team and with a history within law enforcement working on intelligence and fraud related investigations, most of our time is spent on prevention and detection aspects, but also includes time investigating any allegations or suspicion of fraud and corruption.

Risk-ranking exercise

TNT has involved internal departments in its efforts to prevent fraud and corruption, and internal cases have been uncovered and acted upon. Early on, TNT decided to carry out a fraud and corruption healthcheck, which is referred to as the Security Financial Review (SFR), looking at the early indicators of potential fraud and corruption and the associated risks identified. The list was long, and with the benefit of a risk-ranking exercise (creating the TNT Express Fraud Profile) TNT were able to pinpoint the most high-risk items. The eventual result provides a diagnostic report, tailored to the most significant areas of enquiry.

But TNT didn’t stop there

Based on the red flag list, the investigations team started work on plugging the holes – monitoring and measuring the corrective actions taken. Parallel to this the “TNT Integrity Program” was developed with the Group Integrity Department focusing on awareness and dilemma training, in addition to the fraud and corruption



healthchecks. For TNT’s investigation team it has been about having the right things in place and from there focusing on continuous improvement.

Tone at the top

The “tone at the top” is also critical in the program’s success. TNT’s CEO is deeply involved and has taken an active approach. By anchoring it at the top level, embedded by the investigations team and counterparts on the Ethics Committee, the message of ethical transparency and the desired attitudes flows through the business units. The backing of TNT’s CEO and the senior management teams has been crucial to what we have accomplished – it is significant, necessary, and develops the internal culture.

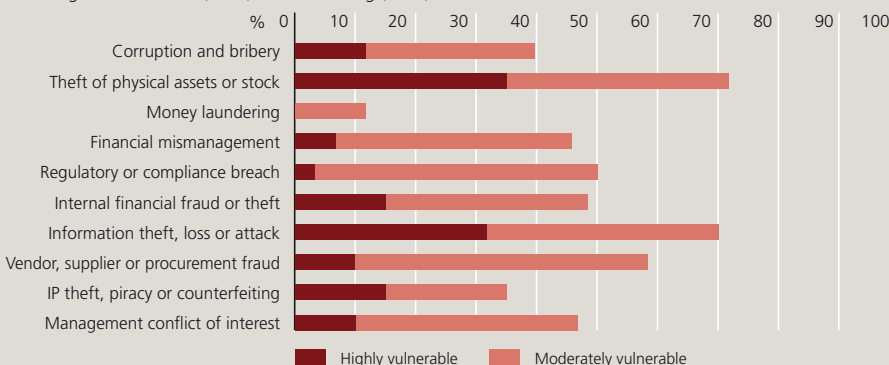
Whistleblower policy

Whistleblowing has also been given attention. It is a well known but unfortunate fact that reporting internal fraud and corruption has historically tended to be a poor career move. In order to succeed with the integrity program, it is of vital importance to establish a whistleblower policy that encourages people to report suspected cases, while recognizing that although the tools and techniques to look for the signs of fraud and corruption are made available, it is essential to give people the confidence to speak out if they suspect any wrongdoing.

The ability to significantly increase profit margins is one compelling reason to systematically manage fraud and corruption risk. A thorough understanding of fraud and corruption risks across the organization is a prerequisite for effective prevention. TNT has impressive risk management and assessment methodology expertise and using the Fraud Profile, they have found that it makes a difference to their customers.

REPORT CARD RETAIL, WHOLESALE AND DISTRIBUTION

- Financial Loss:** Average loss per company over past three years \$3.3 million (41% of average)
- Prevalence:** Companies suffering fraud loss over past three years 86%
- Increase in Exposure:** Companies where exposure to fraud has increased 87%
- High Vulnerability Areas:** Percentage of firms calling themselves highly vulnerable to this type of problem
Theft of physical assets or stock (35%) • Information theft, loss or attack (32%)
- Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud in past three years
Theft of physical assets or stock (67%) • Internal financial fraud or theft (30%) • Financial mismanagement (25%)
Information theft, loss or attack (25%) • Corruption and bribery (22%) • Regulatory or compliance breach (22%)
- Investment Focus:** Percentage of firms investing in these types of prevention in the past three years
Physical asset security (63%) • Financial controls (57%) • Information: IT security (55%)
• Management controls (55%) • Staff training (45%)



Simon Scales is the deputy director Global Security and Compliance for TNT. He has 25 years of experience in both the public and private sectors and has conducted major investigations in Europe, the U.S., South America, China, India, South Africa and the Middle East. Simon has had articles published in many leading newspapers and journals globally.



Reducing retail fraud through background screening

Retail fraud and the struggle against it are nothing new: for decades, businesses have looked for ways to minimize problems such as theft by employees of physical property or of consumer credit and payment information. While technology and training have valuable roles to play here, employment background screening is an effective, simple, and economical measure with which businesses can reduce the risks they face. Screening works because, in many instances, retail fraud is perpetrated either directly by employees or by outsiders receiving their assistance.

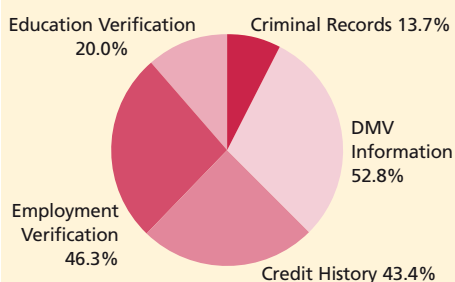
According to the United States Department of Justice, retail companies have a compelling interest in implementing “safe hiring” practices. It calculated that employee theft is the primary cause of 46% of that industry’s losses. Moreover, a Kroll analysis [see box] recently found that more than one in eight employment applicants (13.7%) for jobs in this sector in the U.S. have criminal records.

Lies my applicant told me

Kroll recently performed a US analysis by industry of “hits” – where employment applicants have criminal convictions, motor vehicle violations, discrepancies in employment or education verifications, or derogatory credit information. For 2007, the figures within the retail industry were alarmingly high. For example, 13.7% had criminal records uncovered by Kroll – a number 44% higher than that of other examined sectors.

By thoroughly screening potential employees before they come on board, retail organizations can identify risks from prospective workers before they pose a threat to the business. Criminal histories and falsely stated qualifications are just some of the crucial information that can come to light through a well-executed background check.

Hits for the retail sector 2007



Another useful step is for retailers to integrate ongoing screening requirements for current employees into their employment policy: after all, employees can commit crimes after they start work. By having a structured process to reveal such behavior, employers can more easily be in a position to execute appropriate punitive measures, including possible dismissal.

Effective background screening relies on the following elements:

- **Information sources:** Information should come straight from original sources. Companies should obtain relevant records directly from courthouses, repositories, previous employers, and educational institutions. Similarly, they should ask licensing bodies for details of certifications and credentials.
- **Accuracy:** Investigation methods, data, and final reports used in, or arising from, screening should all be properly reviewed with proven methodologies in order to reduce the likelihood of incomplete, outdated, or inaccurate information being provided to employers.
- **Compliance:** Methodologies used and the type of information acquired in the screening process should be completely compliant with all necessary national, state, local, and industry-specific laws and regulations, such as the United States Fair Credit Reporting Act. Reliable employment screening providers already procure data in strict accordance with these laws and regulations, reporting information that retail businesses can actually use to make legal and effective hiring decisions.
- **Understanding of the retail industry:** Retail businesses should work with a screening provider who can help make decisions about who, what, and how to screen their employees. This requires that screeners understand the specific needs and risks of the sector.

Such a program can go a long way to helping companies avoid making costly hiring mistakes.



Mike Rosen is the president of the Background Screening division of Kroll. Drawing on more than 20 years of experience in the legal profession and employment screening industries, Mike leads the international division of nearly 1,000 professionals in providing innovative screening, due diligence, and fraud solution services.

EIU SURVEY

The financial loss due to fraud has gone up dramatically for this sector in the past year. The industry’s particular problem is with protecting the goods it moves and sells: theft is rampant. Even were this not the case, a variety of other frauds would still present widespread challenges.

- The average loss per company in this year’s survey rose by nearly three-quarters from a year ago – from \$1.9 million to \$3.3 million.
 - A staggering two-thirds of companies have suffered from physical theft in the past three years, up from just under one-half in the previous poll.
 - The sector has ongoing, serious problems with a range of other types of fraud, with roughly one in four firms suffering from each of: internal financial fraud, financial mismanagement, information theft, corruption, and compliance breaches.
- Companies are beginning to understand the extent of their own vulnerability, and are spending more in certain areas, such as physical security.
- 87% of companies believe that their vulnerability to fraud is increasing, up from 76% the year before.
 - 35% now consider themselves highly vulnerable to physical theft, nearly double last year’s figure of 21%, and 32% think the same about information theft, loss or attack, up from just 13%.
 - 84% already have physical security systems in place, but 63% will be spending more on them in the next three years, well up from last year when just 47% expected to make such investments.
 - Overall, more companies in this sector will be putting money into anti-fraud measures than the survey average, especially financial controls (57% to 52%) and management controls (55% to 45%).

A failure to see the big picture may be making the problem worse.

- Despite so many companies feeling more vulnerable, there is apparent confusion about the sector as a whole, with 39% believing that fraud is becoming less prevalent and only 23% thinking that it is increasing.
- High staff turnover (37%) and weaker internal controls, possibly due to cost-cutting (33%), are the two leading causes of increased fraud exposure in the industry. Greater spending on wages to retain staff or on maintaining stronger controls would enhance the anti-fraud investment which sector companies are making.

The retail, wholesale, and distribution sector continues to have a smaller fraud problem in financial terms than most others, and is waking up to its vulnerability to theft. Nevertheless, approaching the issue strategically would make efforts in this area more effective.

Written by The Economist Intelligence Unit



How quickly can you detect a data breach? How will you respond?



A data breach is a legal and technical crisis, and it pays to be prepared, says Alan Brill.

The story is unfortunately all too familiar. A friend of mine received a letter in the mail from his bank. The letter informed him that a data breach of the bank's central computing system had occurred, and that customer information may have been compromised. The letter was sent out to assure customers that they had nothing to worry about, and that the bank was doing everything possible to remedy the situation. This notification made me wonder how often things like this happen, and if there was anything the bank could do to prevent or correct my friend's and the bank's own data breach misfortune.

A cyber-incident can range from a hacker situation, to the loss of intellectual property or identity theft – any instance where data is compromised through the use of a

computer. In this digital age, companies must protect themselves; however, the statistics indicate that this is no small feat.

- A study conducted recently determined that companies spend an average of nearly \$5 million dollars to recover corporate data when lost or stolen. The survey also indicated that the most common methods of data loss include lost or stolen laptops, desktops, PDAs, USB drives, hacked electronic systems, malicious insiders, malicious code and misplaced network storage devices.¹
- A recent UK study found that 132 million sensitive documents are being taken out of UK offices each week on portable devices. The study also concluded that 52% of European employees would take company data with them when they left

their respected company. Even with such high risk for information leakage, the study found that more than a third of European businesses have no set policy for handling sensitive documents, and in cases where policies do already exist, almost a quarter of employees were unaware of the policy.² This situation is not unique to the UK, as similar circumstances abound in U.S. businesses.

So what can organizations do?

It is easy to underestimate the range of potential problems that arise when an organization is faced with a cyber-incident. Some companies respond to a data security breach by deploying their internal IT staff to investigate the matter, and then report their findings to senior management. While this may seem reasonable to the untrained eye, IT staff members are generally not

¹ http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1248216,00.html.
² <http://www.securitypark.co.uk/article.asp?articleid=26423&CategoryID=1>.

equipped with the training and technology to effectively handle these types of incidents. Instead, a better practice is to deploy a computer forensic expert, network intrusion specialist or data breach investigator. With specialized tools that can sift through mountains of system metadata, these trained professionals can

It is not a matter of if an incident will occur, but when. Even one data breach can be catastrophic.

determine the depth of a security breach, recover data that has been corrupted or intentionally deleted, determine how a hacker evaded security checks and perhaps identify the individual who caused the damage. Additionally, these professionals can provide expert witness testimony and reports for the court, should the incident proceed to litigation. They also specialize in identifying methods for plugging the holes in the computing landscape to prevent any future incidents.

Further, it is important to realize that the issues arising from a cyber-incident involve both legal and technical consequences. If you believe a cyber-incident may have occurred, the first step towards effectively dealing with it is to consider the technical aspects. Begin by answering the following questions:

- **What happened or did not happen?**
While at first glance it may appear that an incident has occurred, do not assume this to be true without adequate confirmation. The fear of data loss may spark concern that is not necessarily due.
- **How did it happen?** One must understand the root cause of a breach to effectively remedy the situation. Start by collecting evidence of what happened through custodian interviews, technical inventories, or otherwise, while maintaining a log of your actions. Then, have the evidence analyzed by the proper person on your response team.
- **Who was involved?** A determination of who was involved will assist in correcting the incident and mitigating the possible damages.

A response team must also manage important legal aspects. These may include:

- **What must be reported?** Privacy laws impose a number of obligations on businesses to protect non-public, personally identifiable information.

In the event of a data breach, these organizations may be required to provide notice to the affected individuals.

- **How should potential evidence be preserved?** It may be the case that a breach gives rise to a private cause of action. If it is reasonably anticipated that a court case may follow, parties must suspend routine data destruction practices and immediately issue a document preservation, or litigation hold notice. Your legal team will also need to follow up to ensure proper preservation.
- **What is an appropriate internal and external communication plan?** In an effort to maintain business continuity, a spokesperson must be appointed who is trained in public relations and data breach situations.

Even the most secure organization is not immune from cyber-incidents. Establishing an incident response plan in advance of a crisis, and enabling the incident response team is vital. It is less than ideal to learn to manage a cyber-incident while in the midst of an emergency.

Alan Brill is a senior managing director for Technology Services where he founded the computer forensics practice 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 and developed systems for NASA's Apollo moon landing project. 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 Systems Security Professional (CISSP).

What you don't know can't hurt you?

The Kroll Global Fraud survey shows that information theft, loss, or attack is the type of fraud which most worries respondents, with 25% feeling highly vulnerable, and an additional 47% moderately so.

These figures, however, may underestimate the exposure businesses face. The survey data suggests that those who know more about technology and how it is used day to day in a company have a greater concern.

- Among technology, media and telecom companies, 41% believe themselves highly vulnerable to information attack, by far the highest figure for any risk facing any sector. This figure may reflect the importance of data to this industry's operations, but this sector should also have the most expertise in protecting itself from such risks.
- Employees working below the C-suite who are closer to the everyday technology implementation in the business are over one and a half times more likely than those at the corporate level to see their companies as highly vulnerable (31% vs. 19%).
- Even more striking, Chief Technology Officers, who are in the best position to judge, have opinions closer to those of less senior employees than to those of their C-suite colleagues: 25% see their businesses as highly vulnerable, while only 18% of other corporate executives do.

If senior executives are not worried about their vulnerability to information theft, they should check whether their sense of safety is based on a thorough understanding of the security deployed by the company, or ignorance of the full extent of threat. In this case, too little knowledge could be a dangerous thing.

Using the International Trade Commission in IP investigations



Cross-border intellectual property (IP) investigation can be highly complicated, as the following case study, drawn from Kroll's decades of experience in this field, shows.

Recently, a client approached us with a very complex IP issue, which required a sophisticated international investigation. Executives were concerned that a company in China was violating their process and utility patents and distributing the resultant products worldwide, but they were not sure, and did not know how to fight back even if they were correct.

We started the investigation with an extensive background analysis of the alleged infringer. By digging deeply into corporate records, government filings, media reports, and other available sources of local information, we obtained a detailed understanding of the entity. Next, a deeper probe, involving various source inquiries and site visits, yielded a full picture of how, and through whom, it transacted business. This step is essential, especially in China where firms work through a variety of front entities and sister companies – in this case, one 'sister company' was run literally by a sister of the president of the target entity, who operated at her brother's bidding.

We then had to determine if, in fact, our client's patents were being infringed. Using the intelligence already gathered, we could visit all of the target's manufacturing facilities and obtain samples of their output and waste products. Then, the client's engineers and counsel were able to analyze these to determine that their IP rights were being violated.

We next worked with the client and counsel on a strategy to get the infringer either to stop or to pay a licensing fee for the IP. A review of the target's activities showed significant sales in the United States. We advised filing suit in America's International Trade Commission (ITC), which has the authority to stop intellectual property violators from importing their products into the country. To be eligible to file, our client had to show an appropriate nexus, or tie, with the United States which can often be established by demonstrating some manufacturing or licensing activities there. Indeed, foreign companies are increasingly seeing the benefits of taking this step. In 2002, only 12% of ITC filings were by these businesses, but by 2007 more than 28% were.

The ITC is a powerful weapon because:

- Cases are litigated quickly – usually a Decision and Order is given in twelve to fifteen months, with an Exclusion Order that prohibits further importation of the infringing product possible within two months thereafter; and
- The penalty is so severe, especially if the target already has significant sales in the United States.

Because the ITC acts so quickly, litigation costs can run high. This can be an advantage to filers, however, as it pushes infringers to settle. Our investigation proved very helpful here. Because we had mapped out the target's extensive spiderweb of a distribution network, we could monitor its import levels into the United States over a several year period with great accuracy. This allowed the client to negotiate much more effectively, especially when the infringer claimed to be bringing in only a small portion of the actual amount.

As a result of our efforts, working closely with the client and its law firm, the infringer agreed to enter a license agreement with a substantial up-front payment for prior unlicensed use.

This result might not be appropriate for all situations, especially where the infringing party is a competitor. Then, the IP owner usually seeks an order excluding the infringer from shipping its product into the United States. In either event, an ITC action, supported by Kroll's vast investigative capabilities, may prove an important weapon in your struggle to protect your intellectual assets.



Scott Warren is a managing director in the Tokyo office specializing in protecting intellectual property, computer forensics, e-discovery and anti-cyber crime. Prior to joining Kroll he spent five years at Microsoft as senior attorney and director of internet safety enforcement for North Asia, and seven years as general counsel of Sega Corporation.

EIU SURVEY

Fraud has skyrocketed in the consumer goods industry, taking it from the least affected sector in last year's survey to among the hardest hit this time around.

- The average loss per company over the past three years was \$12.7 million, or over one and a half times the survey average, up from just \$0.6 million or just one-tenth the mean loss to all businesses.
- The number of companies hit by fraud in the past three years has jumped from 68% to 88%.
- A broad range of different fraud has caused the damage: the incidence of physical theft has risen from 39% to 46%, IP theft has gone from 20% to 30%, while procurement fraud, corruption, and management conflict of interest have more than doubled in frequency.
- After healthcare, the consumer goods sector now has the largest range of serious fraud problems. Seven categories affect more than one-quarter of companies.

Awareness of the problem is growing, but not at the same rate as the fraud itself.

- The proportion of companies that consider themselves highly vulnerable, or even moderately vulnerable, has risen in every category of fraud covered in the survey. For the areas of most widespread concern, those who saw information loss as a high risk rose from 9% – an extremely low level for last year – to 19%. For IP theft the equivalent numbers are 11% to 18%.
- Even such rapidly rising concern, however, does not yet reflect the extent of the problem. Only 5% of firms consider themselves highly vulnerable to corruption, even though 26% suffered from the problem in the past three years; similarly with internal financial fraud, just 4% think the risk high, even though 23% have been hit.
- For every category except vendor fraud, a lower or equal percentage of consumer goods companies consider themselves highly vulnerable than the equivalent number for the whole survey.

It is possible that the sector just had a very bad year. With fraud so widespread, however, this can happen even to the best prepared. The industry has spent, and continues to spend, more money than most to combat the problems. The use of almost every type of anti-fraud measure is far more widespread in this sector than elsewhere, and a greater proportion of companies are making new investments in these areas than for business as a whole. On the other hand, the low number of people who think that they are vulnerable may be the root cause of two problems. First, for all the money going into controls, 30% of firms in the sector have weakened them. Second, there is a cultural issue with business implications: fraud will flourish, no matter what the controls, if people are not looking out for it.

Written by The Economist Intelligence Unit

REPORT CARD CONSUMER GOODS

Financial Loss: Average loss per company over past three years \$12.7 million (154% of average)

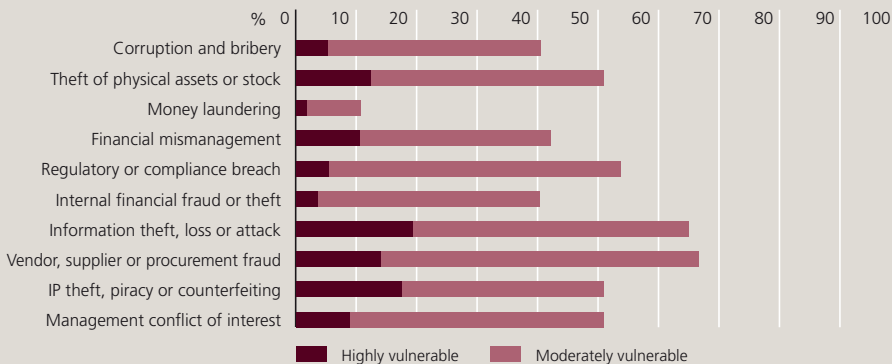
Prevalence: Companies suffering fraud loss over past three years 88%

Increase in Exposure: Companies where exposure to fraud has increased 74%

High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable to this type of problem
Information theft, loss or attack (19%) • IP theft, piracy or counterfeiting (18%)

Investment Focus: Percentage of firms investing in these types of prevention in the past three years
Theft of physical assets or stock (46%) • Vendor, supplier or procurement fraud (33%) • Information theft, loss or attack (32%) • IP theft, piracy or counterfeiting (30%) • Management conflict of interest (28%)
Corruption and bribery (26%) • Regulatory or compliance breach (26%) • Internal financial fraud or theft (23%)

Investment Focus: Percentage of firms investing in these types of prevention in the past three years
Information: IT security (61%) Physical asset security (54%) • Financial controls (51%) • Staff training (51%)
Management controls (47%) • Risk management systems (47%)



Word Power: Linguistic analysis assists fraud investigations



Pete Turecek discovers that the written word can yield great clues.

Intense family pressure was mounting quickly as the wedding date grew closer. The groom's parents told him that his friends had contacted them with frightening allegations about his fiancée's life before he had met her. They provided text from anonymous letters that they had received, as well as other documents that they claimed to have obtained through personal contacts. The parents urged their son to look into the behavior of his betrothed in the country where she had previously lived.

Multiple, detailed analyses of the anonymous letters determined that the writer was an older, Caucasian female, very likely college-educated, who came from upper class society. Using this information and other techniques, investigators found that the author was actually the groom's mother, who was displeased at her son's relationship with a woman of a different race.

Most fraud investigations include the painstaking review of voluminous paper and electronic documents, as well as numerous interviews with possible witnesses and suspects. This activity, combined with a variety of other investigative techniques, typically lets investigators winnow a list of suspects down to a few people, or possibly even one person. In some instances, the tools include a forensic linguistic analysis of written communications which can provide meaningful clues, such as a suspect's profile or the authorship of certain documents.

Every individual's speech and writing style is a combination of various physiological and psychological factors including, but not limited to, gender, age, ethnicity, geographic region, intelligence, education level, and emotional development. Even such personal traits as confidence, shyness, anger, resentment, frustrated desire, and the like manifest themselves in a person's language just as they do in someone's behavior. Moreover, each user

of language – in other words everyone – has personalized characteristic mannerisms with respect to spelling, diction, grammar, semantics, and syntactical usages.

As an example, vocabulary and grammar can sometimes offer indications of geographic or even ethnic origin. Individuals within the same family, cultural group, or geographic region may share many of these particular linguistic habits. Unless quoting someone exactly, however, no two individuals use words, or strings of words, in precisely the same way, whether in speech or in writing. Even for those seeking to disguise their authorship or identity, or to divert the reader's attention, it is actually very difficult to suppress the mistakes or idiosyncratic textual characteristics made innate by learning and life-long usage.

In the case described above, analysts studying the anonymous letters compared them to exemplars from various interested parties and found indications of common authorship in style, phrasing, and content. Linguistic features more typical of females than males were also present, including an expressed reticence to write the letters, and a focus on morality and proper conduct. Comparison of the letters to known exemplars of the mother showed similarities in suppressed effect and exaggerated formality. Based on this careful analysis, along with the results of other investigative activity, the client was able to obtain a clearer understanding of what was going on, and how to handle his family.

While forensic linguistic analysis rarely provides a sole smoking gun in a fraud investigation, it can, in conjunction with other investigative measures, often help to build a preponderance of evidence or assist in providing a more focused investigation.

Peter Turecek is a managing director for business Intelligence & Investigations based in New York. He specializes in Hedge Fund related intelligence, corporate contests and securities fraud.

Common s

The very nature of the hospitality sector's business makes it prone to fraud; it has a material number of human interactions, fragmented services and, frequently, inconsistent policies across companies, to name just a few characteristics which increase risk.

An exhaustive list of frauds in the industry would be impossible, but the following are three common and easily identifiable scams.

Fictitious customer refunds

Incorrect hotel charges to customers can arise from a variety of everyday causes, such as:

- Erroneous billing for services never actually consumed;
- Excessive mini-bar charges – sometimes the result of an automated system recording a transaction as soon as a customer moves a mini-bar item;
- Human error when staff enter the wrong amount into the credit card reader at checkout.

Whatever the reason, refunds for these errors are normally credited to the customer using the same credit card reader that processed the payment during checkout.

In order to process such refunds, most card readers allow the manual entry of a customer's credit card number. Unless strong controls are in place or specific fraud detection tests are carried out, a hotel clerk could credit personal credit cards with regular undetected "refunds" of various amounts. Fortunately, simple daily comparisons of those credit card numbers receiving refunds with those debited at checkout can identify, and help prevent, fraudulent refunds.

Bogus agency commissions

Travel agents are normally paid commissions – ranging from 5% to 15% – on confirmed customer stays which they book. Dishonest employees, however, can carry out the following frauds:

- At check-in, a front desk clerk might deliberately allocate an incorrect code to certain customers so that instead of being classified as "walk-in" – i.e., people who booked directly – they are listed as being booked or recommended by a given agent. The hotel accordingly sends a commission payment to the agent, who then splits the amount with the front desk clerk;
- The clerk can run the same scam entirely to his or her own benefit by registering a bogus agent in the system. More skilled employees may set up an offshore company, thereby reducing the risk of being identified.

Scams in hospitality



Fixed-price menu theft

Hotels often provide fixed-price menus in their restaurants. However, if there is no segregation of duties among staff, fraud can result, as depicted in the following scenario.

A group of four people all order fixed-price menus at \$70 each. At the end of the meal, the waiter brings the bill and puts the \$280 payment in the till. Often, the group leaves the restaurant without taking the receipt, which the waiter pockets. That same evening, if another group of four also orders the fixed-price menu, the waiter can give them the same, already paid bill, and pocket the \$280 rather than running it through the till and into the hotel's books.

None of these schemes may involve large amounts of money, but if they occur repeatedly they can have a highly negative effect on the bottom line.



Stefano Demichelis is a senior director in the London office where he specializes in fraud prevention, detection and internal investigations. He joined Kroll from TNT where he was audit manager for Specialist Services, responsible for identifying risk issues during internal audits, creating fraud detection tests and establishing data mining techniques. Stefano has also worked for TRW Occupant Safety Systems and Arthur Andersen.

EIU SURVEY

Fraud within the travel, leisure, and transportation industry remains a significantly smaller problem than for other industries, but is showing signs of rapid growth both in volume and in the types of activities involved:

- The fraud suffered per company was \$2.5 million according to the latest survey, which is just one-third of the overall average, but more than double the figure from last year's survey.
- The number of companies which suffered fraud of at least one sort in the past three years has gone from 80% to 91%.
- While the incidence of the most prevalent fraud within the sector – physical theft and management conflict of interest – has stayed roughly the same, the frequency of several other types of fraud has risen. Last year, only 3% reported regulatory or compliance breaches in the previous three years but this year the figure was ten times higher at 30%. For information theft, the increase was from 18% to 30%, and for financial mismanagement from 18% to 26%.

With increased fraud has come a greater awareness of vulnerability too, but this is not translating into a wider adoption of anti-fraud measures.

- The proportion of businesses that feel that their exposure to fraud as a whole is increasing jumped from 70% to 85% between the two surveys.
- The percentage of companies that consider themselves highly vulnerable to specific fraud has also jumped across almost all categories, in particular those that have seen a rapid increase in their incidence: for example, for information theft, this figure has gone from 13% to 23%, and for regulatory compliance from 5% to 19%.
- The proportion of companies investing in each of the anti-fraud strategies examined in the survey, however, is very close to that of last year, as the report card shows for the three most widely adopted measures. The only significant exceptions are staff training and due diligence which, although important, cannot solve the problem on their own.

Although still far from the problem other industries face, fraud is growing in the travel sector. Companies need to translate increased concern about the problem into greater action against it if they hope to see such growth reversed.

Written by The Economist Intelligence Unit

REPORT CARD TRAVEL, LEISURE AND TRANSPORTATION

Financial Loss: Average loss per company over past three years \$2.5 million (32% of average)

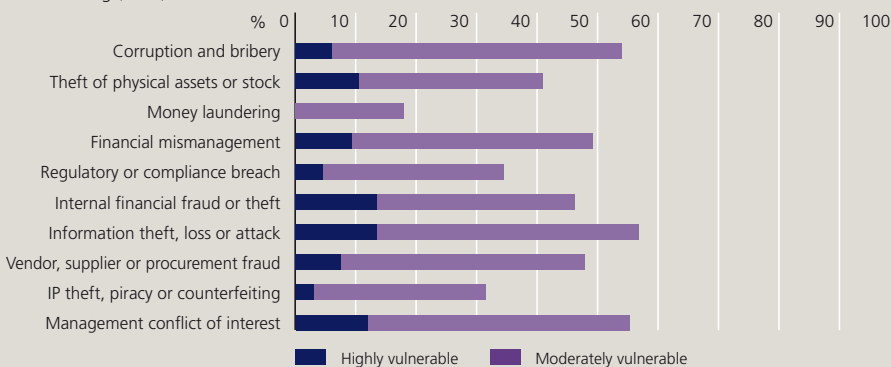
Prevalence: Companies suffering fraud loss over past three years 91%

Increase in Exposure: Companies where exposure to fraud has increased 85%

High Vulnerability Areas: Percentage of firms calling themselves highly vulnerable to this type of problem
Information theft, loss or attack (23%) • Regulatory or compliance breach (19%)

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud in past three years
Theft of physical assets or stock (39%) • Management conflict of interest (30%) • Regulatory or compliance breach (30%) • Information theft, loss or attack (30%) • Financial mismanagement (26%)
Internal financial fraud or theft (25%)

Investment Focus: Percentage of firms investing in these types of prevention in the past three years
Financial controls (61%) • Information: IT security (58%) • Physical asset security (51%) • Due diligence (47%)
Staff training (46%)





Fixed-budget projects:

An automotive company paid more than \$30 million dollars for the construction of a warehouse to store

tires and spare parts. The contract involved a fixed-budget project (FBP) – an arrangement where the price is set at the

start. All seemed to go smoothly; the work was completed on time and within budget.

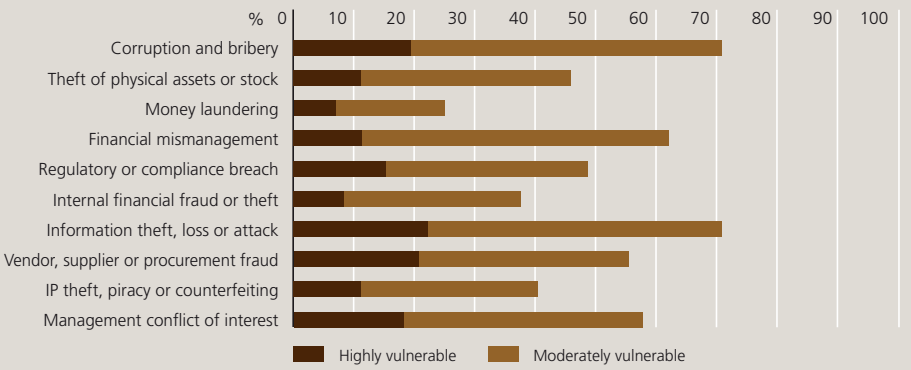
However when the company asked an independent consultant to review the building's blueprints and provide an opinion on whether the cost was in line with market prices, the findings were shocking.

The consultant initially reported that because of the type of goods to be stored in the warehouse, the water reservoir built underneath it and used by its automated extinguishing system would be inadequate in case of fire. Further investigation found that no reservoir actually existed at all; there was only a series of pipes buried in concrete. The site was a fire hazard that would cost the company millions to reach the necessary safety standards.

Many businesses use FBPs to expand facilities at as low a cost as possible. Such arrangements are easier to manage than other kinds of contracts. They can also, to a certain extent, reduce the risks of overruns and abuse on long-term projects. As the above example shows, however, they do contain some hidden challenges.

REPORT CARD CONSTRUCTION

- Financial Loss:** Average loss per company over past three years \$14.2 million (173% of average)
- Prevalence:** Companies suffering fraud loss over past three years 95%
- Increase in Exposure:** Companies where exposure to fraud has increased 85%
- High Vulnerability Areas:** Percentage of firms calling themselves highly vulnerable to this type of problem
Information theft, loss or attack (22%) • Vendor, supplier, or procurement fraud (21%)
- Areas of Frequent Loss:** Percentage of firms reporting loss to this type of fraud in past three years
Theft of physical assets or stock (32%) • Financial mismanagement (31%)
Management conflict of interest (29%) • Corruption and bribery (28%) • Regulatory or compliance breach (26%)
- Investment Focus:** Percentage of firms investing in these types of prevention in the past three years
Financial controls (53%) • Information: IT security (53%) • Management controls (49%) • Physical asset security (46%)



EIU SURVEY

Our survey indicates that damage from fraud in the past three years is now close to a universal experience among construction companies, and the average amount of money lost has risen appreciably. On the other hand, most individual categories of fraud are decreasing in frequency. In other words, what fraud is occurring is becoming much more spread out.

- The average loss per company more than tripled, from \$4.5 million to \$14.2 million, making this the second worst-off sector after natural resources.
- The number of companies where fraud has taken place has also increased from 77% to 95%, the highest prevalence in the survey.
- Some of the most common fraud from the last survey remains as common as before: financial mismanagement and compliance breaches each saw their incidence increase by only 1%, to 31% and 26% respectively. Other categories have grown less common: the incidence of physical theft has dropped from 44% to 32% and corruption from 33% to 28%. Only management conflict of interest has risen appreciably, from 22% to 29%.

The mixed news in the above, however, is masking bigger problems and leading to slightly reduced concern about fraud.

- Although 85% of firms believe that their vulnerability has increased, that is down from 87% last year.
- For most specific types of fraud, the number of respondents who consider themselves highly vulnerable has dropped or stayed roughly the same: for corruption the proportion has gone from 25% to 19% and for compliance breaches 22% to 15%. The only notable exceptions are management conflict of interest and IP theft.
- The number of companies in this sector investing in new anti-fraud measures is only about the same as the survey average, despite the elevated losses and number of companies hit.

Despite a few successes in specific areas, the construction sector has a big fraud problem, and needs to address it more aggressively.

Written by The Economist Intelligence Unit



hidden risks

While each construction project is unique and faces a wide variety of possible frauds, the following are common abuses that companies opting for FBPs might encounter:

- A faulty tendering process may occur when different construction companies are part of a bigger conglomerate and collude to make the “best offer” more expensive than necessary.
- An incomplete FBP agreement which does not include certain parts of the project in the price – for example maintenance or special electrical cabling – is a way for builders to drive up their overall charges.
- The material used might differ in quantity and quality from what was agreed. For instance, the appropriate type of concrete for a project depends on factors such as the size of the building and the typical weather conditions it will face. The higher the quality of the concrete, the greater the cost for the builder. Unscrupulous companies might use poorer quality, less expensive concrete than contracted for, which could affect the structure’s stability.
- Managers who are aware of likely future changes in a project – a common occurrence in construction – might collude with a bidder, encouraging it to submit a fictitiously low offer. Once the project is awarded as an FBP, the construction company can then charge excessively for any requested changes, allowing it to make unduly high profits.
- When a construction company carries out concurrent projects that are not all FBPs, the risk of costs being “diverted” from FBP to non-FBP sites is very high.

This partial list shows that hidden frauds in construction can have serious long-term consequences. The fact that costs appear to be fixed is no reason not to question them.



Stefano Demichelis is a senior director in the London office where he specializes in fraud prevention, detection and internal investigations. He joined Kroll from TNT where he was audit manager for Specialist Services, responsible for identifying risk issues during internal audits, creating fraud detection tests and establishing data mining techniques. Stefano has also worked for TRW Occupant Safety Systems and Arthur Andersen.

Blowing hot and cold: Target

What threats should companies in particular sectors look out for? There is no easy answer: every business has a unique risk profile, dictated by its customers, operations, locations, assets, suppliers, and many other factors. Nevertheless, common issues within sectors give companies looking to address fraud some starting points and help to indicate likely areas of risk.

Like last year, we have analyzed the survey results to create a heat map, looking at the frequency of loss for each sector from specific fraud areas. We have matched this information with data on the average size of loss. We also analyzed the perception gap: the difference between the sector's perception of vulnerability and the reported loss. The sectoral highlights are:

Financial services:

A high threat from money laundering, financial mismanagement, and regulatory or compliance breaches. High average level of loss.

Professional services:

The most prominent issues are a moderate threat from information theft or loss, and (to a lesser degree) money laundering and conflict of interest. Low average level of loss.

Manufacturing:

A diverse threat (in part because we have defined this sector widely) from corruption, theft, vendor/supplier fraud, and IP theft. Moderate level of loss.

Healthcare, pharmaceuticals and biotech:

A high threat from regulatory and compliance breaches, with moderate threats from vendor/supplier fraud and IP theft. Moderate level of loss.

Technology, media, and telecoms:

A high threat from information theft or loss, and a moderate one from IP theft. Moderate level of loss.

Natural resources:

A high threat from management conflict of interest and corruption. High average level of loss.

Travel, leisure, and transport:

A very diverse range of moderate threats, including information theft or loss, regulatory and compliance breaches, financial mismanagement, money laundering, and conflict of interest. Low average level of loss.

Retail:

A high threat from theft of assets and stock, and internal financial fraud. Low average level of loss.

Consumer goods:

This sector reported surprisingly high levels of threat across the board, especially for IP theft, vendor/supplier fraud, information theft or loss, and corruption. Moderate level of loss.

Construction:

High threats from corruption and financial mismanagement. Moderate level of loss.

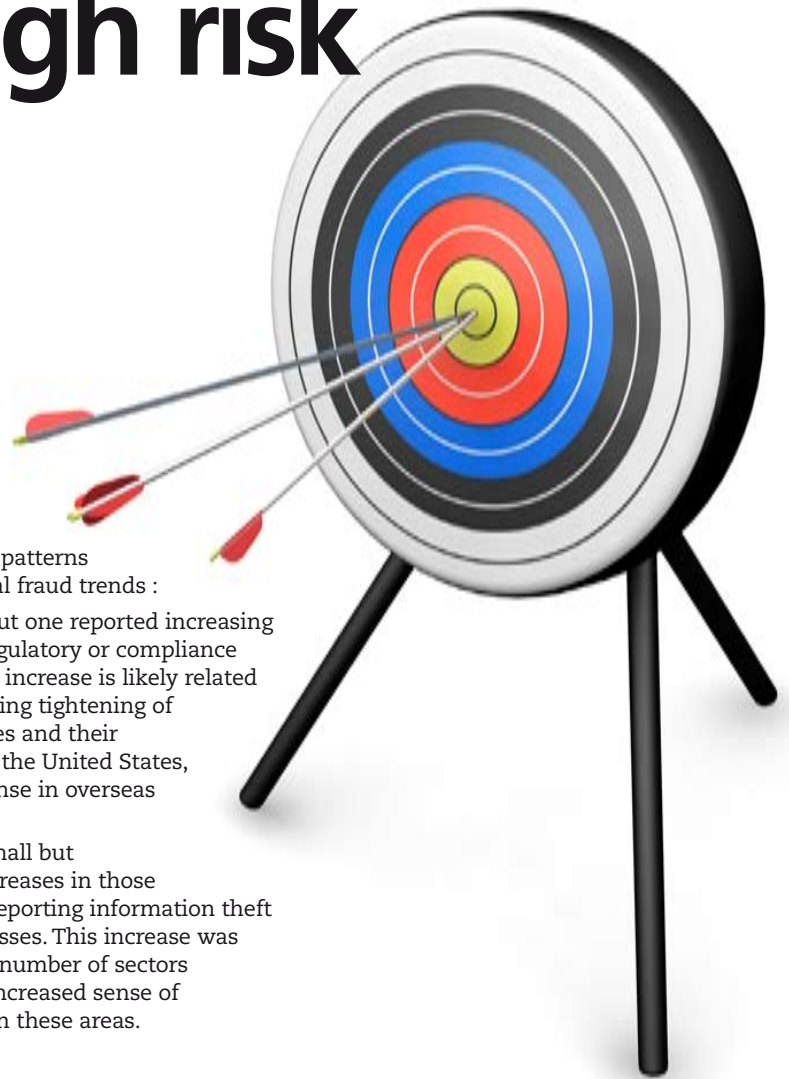
| Areas of frequent loss 2008 | Financial services | Professional services | Manufacturing | Healthcare, pharmaceuticals & biotechnology | Technology, media & telecoms | Natural resources | Travel, leisure & transportation | Retail, wholesale & distribution | Consumer goods | Construction |
|---------------------------------------|--------------------|-----------------------|---------------|---|------------------------------|-------------------|----------------------------------|----------------------------------|----------------|--------------|
| Corruption and bribery | 15.8% | 15.3% | 23.5% | 20.3% | 13.9% | 26.0% | 19.3% | 21.7% | 26.3% | 27.8% |
| Theft of physical assets or stock | 27.2% | 22.9% | 52.9% | 40.5% | 32.7% | 39.0% | 38.6% | 66.7% | 45.6% | 31.9% |
| Money laundering | 12.3% | 2.8% | 0.0% | 0.0% | 2.0% | 5.2% | 7.0% | 1.7% | 1.8% | 5.6% |
| Financial mismanagement | 28.9% | 15.3% | 16.5% | 25.7% | 17.8% | 26.0% | 26.3% | 25.0% | 12.3% | 30.6% |
| Regulatory or compliance breach | 35.1% | 16.0% | 27.1% | 36.5% | 19.8% | 19.5% | 29.8% | 21.7% | 26.3% | 26.4% |
| Internal financial fraud or theft | 23.7% | 9.0% | 14.1% | 24.3% | 8.9% | 24.7% | 24.6% | 30.0% | 22.8% | 16.7% |
| Information theft, loss or attack | 23.7% | 29.2% | 22.4% | 25.7% | 32.7% | 28.6% | 29.8% | 25.0% | 31.6% | 15.3% |
| Vendor, supplier or procurement fraud | 7.9% | 15.3% | 24.7% | 24.3% | 13.9% | 18.2% | 17.5% | 18.3% | 33.3% | 19.4% |
| IP theft, piracy, or counterfeiting | 8.8% | 12.5% | 17.6% | 21.6% | 21.8% | 16.9% | 12.3% | 13.3% | 29.8% | 11.1% |
| Management conflict of interest | 24.6% | 27.8% | 14.1% | 28.4% | 20.8% | 39.0% | 29.8% | 16.7% | 28.1% | 29.2% |

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

ing areas of high risk

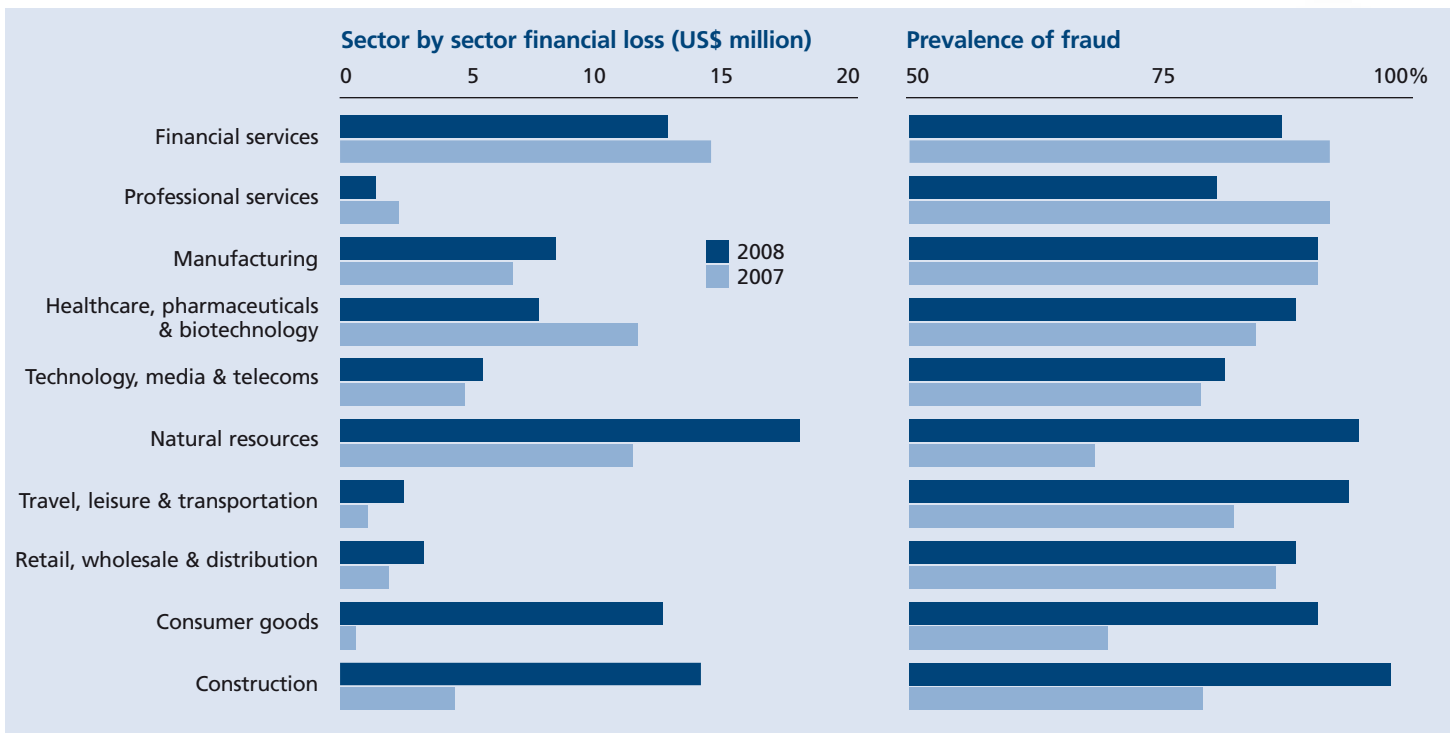
We used similar techniques to analyze changes in fraud patterns revealed by the survey, examining areas where sectors report significant increases in loss:

- The biggest change is an increased loss across the board in the consumer goods sector, which reported markedly higher levels of most of the fraud categories about which we asked. It is not clear from the data whether this represents a significant deterioration in this sector's problems or some other fluctuation in the data from last year. Interestingly, the consumer goods sector had the biggest apparent gap between perceived vulnerability and reported loss.
- There was a marked increase in loss reported by the natural resources sector, including in financial mismanagement, IP theft, and information theft. This increase is related to the continuing rise in oil prices and the industry's shift into higher-risk areas.
- The healthcare, pharmaceuticals, and biotechnology sectors reported increased problems with corruption and theft of assets and stock.
- The travel, leisure, and transportation sectors reported increased problems with regulatory and compliance breaches and information theft or loss.



There were also patterns reflecting general fraud trends :

- Every sector but one reported increasing issues with regulatory or compliance breaches. This increase is likely related to the continuing tightening of regulatory rules and their application in the United States, and the response in overseas jurisdictions.
- There were small but significant increases in those respondents reporting information theft and IP theft losses. This increase was matched by a number of sectors reporting an increased sense of vulnerability in these areas.



North America**Consulting Services**

Dave Holley
Boston
617 421 0517
dholley@kroll.com

Michael Fellner
Chicago
312 681 1500
mfellner@kroll.com

Ken Mate
Los Angeles
213 443 1103
kmate@kroll.com

Blake Coppotelli
New York
212 833 3487
bcoppotelli@kroll.com

Bill Nugent
Philadelphia
215 568 8090
bnugent@kroll.com

John Slavek
Philadelphia
+1 215 568 8313
jslavek@kroll.com

Dave Hess
Reston
703 796 2880
dhess@kroll.com

Betsy Blumenthal
San Francisco
415 495 2200
bblument@kroll.com

Kroll Ontrack

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

Identity Theft

Brian Lapidus
Nashville
615 320 9800
blapidus@kroll.com

Background Screening

Scott Viebranz
Nashville
615 320 9800
sviebranz@kroll.com

Latin America**Consulting Services**

Sam Anson
Miami
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

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

Legal Technology

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

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

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

Background Screening

Tony Shepherd
London
44 20 7029 5418
tshepherd@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 3,800 employees and serves a global clientele of law firms, financial institutions, corporations, non-profit institutions, government agencies, and individuals. Kroll is a subsidiary of Marsh & McLennan Companies, Inc. (NYSE: MMC), the global professional services firm.

Experts in fraud intelligence and investigations

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

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

Kroll also provides services in

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

www.kroll.com

KROLL

