



Attacking the proceeds of crime

At this year's annual CCS lecture, **Paul Evans** offered a fascinating insight into the measures the UK's Serious Organised Crime Agency (SOCA) uses to destabilise criminals, reduce the harm they do and part them from their ill gotten gains.

Established in 2006, SOCA has developed its own innovative responses to tackle the changing criminal landscape, using intelligence and enforcement activity to detect, disrupt and dismantle organised criminal networks in the UK, and reduce the harm they do to individuals and communities.

The agency's rapid evolution to deal with the changing picture of organised crime has necessitated development of a new approach and the introduction of several new techniques that have been supported and augmented with the granting of new powers that enable SOCA to be more effective, efficient and successful.

Paul Evans, SOCA's Director Intervention, spoke at length about this during his presentation, and

the former Chief of Investigations at HM Customs began by asking the audience what they thought organised crime looks like. This was his problem when he started, he said. He didn't have an answer and nor did many others, yet they knew from the numbers that it was getting worse and that something drastic needed to be done. The question was what?

Taking mass marketing fraud – lottery scams, advance fee frauds etc - as an example, Mr Evans explained SOCA's 'different' approach to an organised crime that the Office of Fair Trading estimates costs UK victims around £3.5 billion every year. Working with others, it devised a strategy that aimed to disrupt and dismantle the activities of some of these groups, which also included measures to increase



The payback logo is part of a multi-agency approach to taking the cash out of crime.

awareness of the threat and encourage innovation to tackle it. A key strand of this strategy was to intercept mass market fraud re-mailing letters and close down the 'address' they had been sent to. Then it wrote to every one of the victims explaining they had been tricked, returned their 'investment' and advised them to think carefully before responding to unsolicited mail of the same type in the future.

Continued on page 2/

The SOCA strategy:

1. To build knowledge and understanding of serious organised crime, the harm it causes, and of the effectiveness in tackling it.
2. To tackle criminal finances and profits including through asset recovery.
3. To increase the risk to serious organised criminals operating against the UK, through traditional means and by innovation within the law.
4. To collaborate with partners, join up domestic and international efforts to reduce harm and provide high quality support to our partners; and as appropriate seek theirs in return.
5. To build the capability to make a difference.

In This Issue of CCI

CCS LECTURE

- New UK bribery law explained 4
- Combating UK money laundering 5

BANK SECURITY

- End of the line for tax havens? 6

FRAUD

- Indonesia's new investor blacklist 8
- \$1.5bn pharmaceutical fraud 9
- Due diligence checks on the rise 10

PIRACY

- Somalia's winners and losers 11

CORPORATE SECURITY

- The security/privacy paradox 14
- The rise of insider snooping 16

Attacking the proceeds of crime - from page 1

Finally, the agency letter provided contact details for further advice and guidance.

What criminals want

Thinking further outside the box in its bid to find out what to do about organised crime, SOCA decided it needed to find out what criminals want and, importantly, what they feared if discovered that the only risk they were really concerned about was losing their assets.

With money comes the temptation to spend it; to acquire assets, either to live it up or plan for the future, or simply to legitimise it. The moment criminals do this their risk of detection increases. These people, who behave normally most of the time, have to break cover to acquire assets and most are apparently as susceptible to fear, uncertainty and doubt as anyone else.

This gives SOCA the opportunity to confirm its suspicions and make a breakthrough. It holds a large number of records on individuals involved in organised crime that it checks on a regular basis it can spot changes in lifestyle and/or behaviour that can become the catalyst for a more detailed investigation. And once assets with dubious provenance are identified it has a powerful array of tools at its disposal to seize them.

“Building knowledge,” says Paul Evans, “is SOCA’s principle strategic priority and will underpin everything else we do. Information is the key to removing criminal assets, increasing the risk to criminals, developing partnerships and building capabilities. By investing we improve our understanding, and once we understand what criminals want and how they work we can prioritise the right tasks for action and deploy the most effective and proportionate tools available,” he adds.

Intervention capabilities

Outlining some of these tools, and noting that SOCA’s international network currently comprises 140 officers in 41 countries who work closely with local authorities amongst its 3,200 staff, Mr Evans said the agency relied heavily on partnerships with other organisations to get the job done. In particular, he mentioned the creation of the Organised Crime Partnership Board (OCPB), through which the agency, HM Revenue & Customs, the UK Border Agency and the Police have put in place systems for sharing details of the organised criminal groups known to each group and agreed a series of joint programmes to tackle them.

Supporting this, it has at its disposal legislation such as the Proceeds of Crime Act 2002,

Serious Organised Crime and Police Act 2005, and Serious Crime Act 2007, which are proving useful allies alongside SOCA’s merger with the Assets Recovery Agency last year that now puts it at the forefront of recovering criminal assets and disrupting organised group finances.

Mr Evans made particular reference to the new civil recovery arrangements contained within the Serious Crime Act and said the agency was making good use of its provision of Serious Crime Prevention Orders (SCPOs), which at a stroke remove processes that could previously take up to two years to litigate. SCPOs can be obtained by the prosecution after conviction, or without prosecution through the High Court, and are designed to make it more difficult for ‘bad’ people to harm citizens. Illustrating their usefulness, Mr Evans described how tax could be levied on an asset at 40% plus a 40% penalty, thereby causing 80% of the value of an asset to disappear virtually overnight by just filling out a few forms. This is a huge shock to any criminal who values his assets above all else.

In relation to harming citizens he also referred to SOCA’s Harm Framework, a useful reference which characterises the harm caused by organised criminal activities in ‘real

The Annual CCS Lecture once again provided delegates with excellent networking opportunities



world' terms by type and scale – physical, social, environmental, economic and structural. He said this framework was now used in decision-making for prioritising tasks and as a means of ensuring the operations the agency undertakes deliver the benefits envisioned.

Other asset recovery tools include Suspicious Activity Reports (SARs), which Mr Evans noted have been under-utilised, Financial Reporting Orders (SOCA currently has 65 in force that require the individual to set out details of income, assets and expenditure at regular intervals) and 'co-operation agreements' which encourage people to tell how they committed a crime in return for time off their sentence.

Using SARs

Expanding the point about the underuse of SARs, he explained how SOCA has been able to create a SARs hotspot map and use this to mount specific operations. One such Operation was carried out in a UK provincial city which apparently has more car dealers per capita than anywhere else in the UK. Renowned as a centre for the heroin trade, the area generated a number of SARs as attempts were made to launder the proceeds of criminal activity. SOCA, working with HMRC and local police set out to tackle the infrastructure supporting organised crime in this city, and in turn to reduce the harm the heroin trade was doing to its citizens.

It targeted the huge number of MSB's (money service bureau) in the city, most of who were unlicensed and shut them down, reducing the dealers' money laundering opportunities. It got records of those buying expensive new cars and discovered many owners had not bothered to tax or insure them. 46 luxury cars have been confiscated and crushed so far. Then it went after the car dealers and put many out of business. Finally, it produced a leaflet notifying local residents that SOCA officers were working in their community to reduce safety issues and provide reassurance.

Mr Evans says the response to this initiative was very positive. "Only now are we starting to see many of the things originally envisaged in the Proceeds of Crime Act starting to materialise," says Mr Evans.

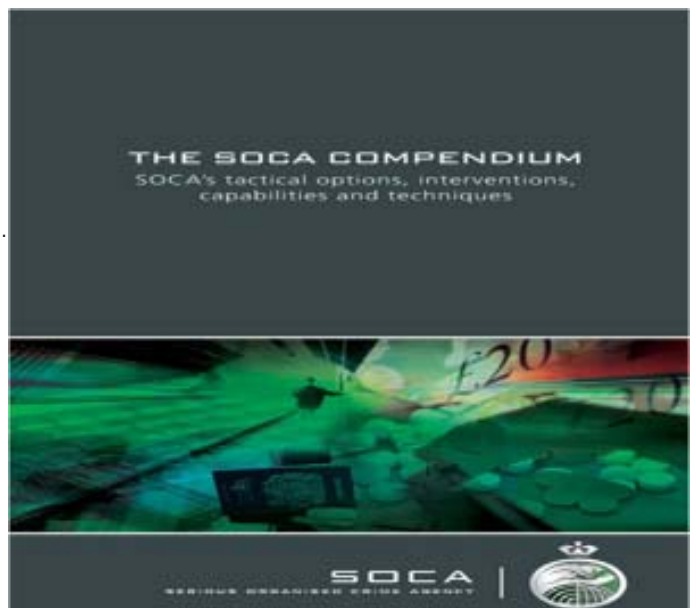
"This, together with the other legislation, means we can now virtually throw the kitchen sink at organised criminals. At the same time, civil recovery is really starting to take off. I believe what all this means for UK criminals is that life is going to change.

"Our approach and the measures we have introduced to support it is helping to turn the enforcement process 'inside out'. Latest intelligence indicates a discernable anxiety amongst some organised criminals about SOCA's focus on criminal assets. Our aim now is to turn this anxiety into outright fear."



Newspaper report detailing one of SOCS's recent successes

The SOCA Compendium contains a list of all the tools that enable UK law enforcement to constrain the activities of organised criminals.



UK steps up bid to get to grips with bribery

*The publication in March this year of the new UK draft Bribery Bill has provoked plenty of interest and comment on its bid to reform the criminal law. Its purpose is to provide a new, modern and comprehensive scheme of bribery offences that will enable courts and prosecutors to respond more effectively to bribery at home or abroad. Ahead of this year's CCS lecture, **Eoin O'Shea**, a Partner at lawyers Lawrence Graham LLP, presented an overview of the new Bribery Bill and assessed its potential.*



Eoin O'Shea

The fight against bribery is the fight for fair international trade and overseas development - it supports access to justice and open markets, and is a crucial part of efforts to reduce global poverty.

The World Bank estimates that £1,000 billion (\$1 trillion) worth of bribes are paid globally each year. Bribery adds up to 10% to the total cost of doing business globally and up to 25% to the cost of procurement contracts in developing countries. Many of the negative effects of corporate corruption were reviewed by Lawrence Cockcroft, the Chairman of Transparency International UK, in the 2008 Annual CCS Economic Crime Lecture.

The draft Bribery Bill, part of a comprehensive UK government strategy to fight bribery, is designed to allow the UK to collaborate more effectively with its international partners in tackling corruption around the world. Its aim is to transform and simplify the law, replacing old and fragmented legislation with a clear and consolidated statute. It will enable police, prosecutors and courts to take effective action against bribery, whether at home or abroad.

The draft Bill proposes a complete code that effectively makes all previous legislation on the subject, some of it dating from 1896 obsolete. Existing statutes are to be repealed, common-law offences abolished and the previous definitions of bribery redefined. Two new offences are also proposed: the negligent failure of a commercial

organisation to prevent bribery (subject to a 'due diligence' defence); and bribery of a foreign public official. UK jurisdiction is extended to all persons and companies with a UK connection (including those in UK overseas territories), 'facilitation payments' are not tolerated, there is no distinction between 'public' and 'private' bribery, and there is no longer any requirement for the Attorney General's permission before the Crown can prosecute. The proposed penalties are also stricter: 10 years in prison and an unlimited fine if convicted on indictment.

General offences

Looking at the two new General Offences contained in the draft Bill, a payment offence is committed when a person offers, promises or gives financial or other advantage to another, intending to induce improper performance of the other person's functions. The functions are those subject to an expectation of impartiality/good faith/trust. It is also an offence to offer, promise or give an advantage in circumstances where one knows acceptance would in itself be a breach of the expectation of impartiality etc, outlined above.

A receiving offence is committed when the receiver agrees to receive or accept a financial or other advantage: intending to be thus influenced into improper performance of the function subject to the expectation of impartiality etc outlined above. As above, there are circumstances where even a request or receipt of an advantage is itself

improper without more (for example a Judge accepting payment from a litigant). The proposed law also criminalises request, receipts etc as a reward for past impropriety, as well as circumstances where the receiver performs the function improperly in anticipation of advantage.

The new offence moves away from the agent/principal model which underlay much of the old law. It is based on the normative expectation that a public official or company officer or employee will act impartially and in good faith and fulfil his/her requirement of trust. It thus focuses less on the legalities of a person's status and more on examining a person's functions and responsibilities, and how they are performed.

Corporate offences

The Bill would introduce an entirely new offence on corporations (including partnerships). The essence of the offence is the negligent failure by a company to prevent bribery. An offence would be committed when a person who provides services for a company - such as an employee or agent - pays a bribe in connection with that company's business, and a "responsible person" within that company negligently fails to prevent the bribe.

A 'responsible person' would be someone who is employed by the

UK must mount a stronger defence against money laundering

THE UK may have done much to tighten up its efforts against money laundering and to combat the financing of terrorism recently, but a new report from Transparency International UK has revealed that more flaws still exist.

The report 'Combating Money Laundering and Recovering Looted Gains' looks at the complex legal and regulatory armoury the UK employs to counter money laundering. It focuses on how robust the UK's current defences are against money laundering, what should be done to strengthen them, and how – once those defences are breached – the UK should cooperate promptly to ensure looted funds are returned to the victim countries.

Noting that once mingled with funds in a large financial centre like London, dirty money – whether the proceeds of looting by corruption, procurement bribery or other criminal activities – is easier to launder, the report says that in the current system:

- A corrupt foreign politician can still stash stolen money in a UK bank account
- Trusts and shell companies can still be used to launder dirty money
- The UK's Overseas Territories can still provide havens for the proceeds of corruption.

The report makes several key recommendations to close the gaps it identified, namely:

company with functions including the prevention of bribery, or, if there is no such person, any senior officer of the company. A senior officer is presently defined as a director, officer, manager, secretary or other similar, or a partner or person with control or management (if the company is a partnership). However, this definition is seen by many as very wide, and it may be cut down in the final legislation.

Corporate bodies charged with this offence may be able to rely on a defence – that of adequate procedures. If a company can prove it had adequate procedures designed to prevent bribery in place then the defence will apply, unless the negligence in failing to prevent (the payment of a bribe) is that of a senior officer.

It is not quite clear what procedures are 'adequate', and whatever they

are why any senior officer should want to concern himself with them, since if he does so but fails to prevent bribery it may deny the company the adequate procedures defence. The effect of this provision may, in fact, be to discourage senior officers of companies to engage themselves with bribery and anti-corruption policies, and thus relegating these to the lower echelons of corporate priorities.

Finally, there is a section regarding the bribery of foreign public officials (FPO). The provision of advantage to a FPO: a) which is intended to influence the FPO in their function, and b) which is intended to obtain/retain a business advantage, and c) which is not legitimately due to the FPO, is an offence.

Of course, what is legitimately due remains a question of foreign law in the country where the payment

is made. The provision would make it incumbent on those doing business overseas to satisfy themselves as to the detail of local laws in all circumstances where they are making payments to government officials or offices.

Whilst the Bill has yet to be tested by real-world situations, O'Shea believes it has an inherent flexibility to resolve many of the problems it is trying to address.

Overall, however, O'Shea believes the draft Bribery Bill is a positive step forward and, if enacted, marks a radical change in English law in this area. It should equip the authorities with at least some of the tools they need to go after overseas and domestic bribery. Compliance with the new law, once enacted, will require some thought and some work by businesses who will need to comply with it.

On preventing money laundering

□ The UK government should work with its smaller Overseas Territories (OTs) to ensure their financial centres and enforcement authorities have the necessary resources and capacity to prevent money laundering. If not, the UK should either invest in boosting their capacity or wind down weak OT financial centres.

□ Tighter systems to reinforce the efforts of UK banks and other institutions in identifying and doing due diligence on their high-risk customers – ie those whose profiles suggest they may be money launderers.

□ The establishment of a central database of other countries' domestic restrictions on asset ownership by their citizens that could help UK institutions more easily identify customers who have breached those restrictions and are likely to be corrupt.

On more effective UK help for foreign countries in recovering stolen funds

□ The UK should do more to help return recovered stolen funds to their rightful owners, particularly through civil (as opposed to criminal) recovery routes.

□ A Memorandum of Understanding between all the UK organisations involved in combating money laundering and recovering stolen money should be agreed, aimed at improving co-operation and speeding up the process.

Continued on page 6/

Faced with a global recession caused partly by commercial financial crime, governments have been pushed into taking action against tax evasion in recent months by ending the practice of banking secrecy. Is it the end of the road for tax havens as protected jurisdictions where illicit transactions can hide?
Alan Osborn reports.

UK money laundering - from page 5

- The UK should cushion the high cost of asset recovery for claimant states by supporting an international trust fund or providing loans and grants to meet those costs – which would be repaid once the stolen assets are released.
- The UK should be more proactive in raising awareness of its asset recovery process among foreign countries to address current confusion and uncertainty.
- The Department for International Development (DFID) should help developing countries increase their capacity for asset recovery - including investment in recovery specialists.

Commenting on the report, Chandrashekar Krishnan, Executive Director of TI-UK said: "The UK cannot rest on its laurels. It is the world's largest financial centre and is therefore vulnerable to reputational damage from allowing dirty money to circulate. Giving looted foreign funds a safe haven in this country only attracts more to its shores. That's why the UK's defences against dirty money must be robust and – if those defences are breached - an energetic and proactive system should be in place for repatriating looted funds."

Tax havens are under fire - But are they finished?

History may well judge that the era of international tax havens came to an end in the first few months of 2009. This is a bold claim and its truth (or not) may not be known for a year or more yet, but what can be said is that the crackdown on tax evasion and tax avoidance (as on money laundering and other financial crimes) has suddenly and surprisingly taken a much higher profile in recent months. The key is the astonishing surrender of banking secrecy by financial centres that until this year safeguarded it with every means open to them.

Those who attended a briefing by tax officials at the Organisation for Economic Cooperation and Development (OECD) in Paris in June to review the think-tank's work in countering tax evasion were left in no doubt of the dramatic changes. "We've seen more progress in the last six months than in the past 30 years," said a senior official.

"Look at what's happened: countries like Andorra, Liechtenstein and Monaco resisted to the bitter end and have now finally seen the light. Look at Singapore and Hong Kong - major financial centres outside the OECD - they've now committed. Inside the OECD we had four countries with strict banking secrecy - Austria, Belgium, Luxembourg, Switzerland - but they have now removed all their reservations. In the last four months we've seen 40 'tax information exchange agreements' (TIEAs) – half of the total signed since 2000 and every single week there are new ones. It's been absolutely amazing."

As the OECD noted, "since the beginning of 2009, international tax evasion and the implementation of the internationally agreed tax standard has been very high on the political agenda, reflecting recent scandals that have affected countries around the world, the spotlight that the global financial crisis has put on financial centres generally, and the recent G20 London Summit." One might wish to add to this the election as US president last November of Barack Obama who has consistently opposed tax havens and banking secrecy.

This all bore fruit at the London G20 meeting in early April when the 20 government leaders agreed a number of initiatives against tax havens "on the issues of lack of transparency and lack of exchange of information." The main work to develop this is being carried out by the OECD, whose membership is the 30 leading industrial nations but whose Global Forum on Taxation lists 84 jurisdictions pledged to sharing tax information.

Calls for more

Not everybody agrees that the proposed OECD measures are strict or comprehensive enough though. John Christensen, director of the International Secretariat of the Tax Justice Network (TJN), says the proposals are "very welcome - but there is a big however." In particular the measures proposed for information exchange "are frankly timid and ineffective and we say they need to be much more ambitious," he said.

The TJN is an organisation of economists and financial professionals formed to promote transparency in international finance and to oppose secrecy.

Auction rate securities settlements

BANK of America, RBC Capital Markets, and Deutsche Bank have agreed to pay about \$6.7 billion to settle SEC charges that accused the financial firms of lying to investors about the risks of auction rate securities.

Under the terms of the settlement the three firms will pay nearly \$6.7 billion to about 9,600 customers who invested in the high-risk securities before the auction rate securities market froze in February 2008.

According to the SEC, Bank of America, RBC, and Deutsche Bank told prospective investors that auction rate securities were highly liquid investments and just as safe as cash. In late 2007 and 2008, with the worldwide market for the securities crumbling, the banks continued to push the investments on clients who did not know the status of the market, the SEC said. The banks also were accused of failing to inform their clients of the risks before leaving them high and dry when the auction rate securities market froze.

Now Bank of America is to pay \$4.5 billion, Deutsche Bank \$1.3 billion, and RBC \$800 million to former clients who lost money in the investments. In addition, under the settlement agreed last month each firm will offer to purchase auction rate securities at par from individuals, charities, and small or medium businesses that purchased the securities from the firm, even if those customers later moved their accounts to another firm. They will also pay eligible customers who sold their auction rate securities below par the difference between par and the sale price of the securities.

Mr Christensen explained that the OECD was proposing information exchange "by request" which would require the complainant to apply to the courts of the target country "with a smoking gun."

He told Commercial Crime International that the TJN much preferred the EU model of "automatic information" when bank account information is automatically provided to other EU countries. This was "a very effective deterrent and needs to become the global model," he said. TJN has been asked by the G20 countries to produce a model for a global multilateral information exchange.

TJN is also pressing for a 'country-by-country' reporting system for multinational companies under which separate accounts would have to be published for each country rather than consolidating everything in one set. "This will make more transparent how they hide their internal profit-shifting arrangement to shift profits out of 20 countries where they are created and into tax havens," Mr Christensen said.

Dr Ian Roxan, senior lecturer in law and director of the tax programme at the London School of Economics, said the 'on request' agreements "typically contain provisions to limit the application of bank secrecy rules and to include disclosure of the ownership chain of a local company, where the local company has the information."

He said this meant that their effectiveness depended to a significant degree on the investigative efforts of the countries seeking information. "Tax havens may well be able to resist providing information for something that they can characterise as a fishing expedition," he said.

Approach too narrow

The OECD approach was also described as "narrow" by Ms Maylis Labusquiere, policy officer for Oxfam France, who noted that it required only 12 TIEAs for a country to move from the 'grey' (action promised but not implemented) to the 'white' (fully implemented) list and this was too few. She also called for an end to secrecy over the real owners of trust funds which were increasingly being used for tax avoidance.

Oxfam France recently published a study showing that developing countries were losing out on up to \$124 billion every year in lost income from offshore assets held in tax havens.

These are valid points but scarcely invalidate what an OECD official calls a "sea change" in attitudes towards banking secrecy in recent months. Will the new openness and cooperation really put an end to tax evasion?

"We've made great strides but we haven't yet eliminated every loophole and it may be impossible to do so," said Peter Skinner, a Labour MEP who sits on the European Parliament's economic and monetary affairs committee. "It's always been impossible to eliminate fraud because one fraud has always been replaced by another. We need not just cooperation but use of the same standards, the same regulatory approaches everywhere and if we don't get that there'll always be loopholes," he said.

Most experts however believe that tax evasion using offshore companies will fall sharply under the impact of the new disclosure requirements.

While there may be hold-outs for a while, "they will be increasingly isolated and disreputable" said an OECD official. "In this respect at least we can look forward to a more honest world," he added.

Indonesia steps-up investor protection in response to recent frauds

INDONESIA's Stock Exchange (IDX) says it plans to regularly publish a list of investors and brokers with 'questionable' track records. The move is part of new measures to help prevent fraud in the capital market and provide greater protection for the investing public. The country currently has almost one million individual investors, who are served by a total of 119 securities houses.

The new IDX blacklist will be made available online and will be used as a form of early warning to help stock market authorities and securities houses detect potential scams in the capital market. It is to be based on reports - from fellow investors or brokers - about possible wrongdoings, but will only be accessible to securities companies with a password. Public access to the list will be allowed, but only when any allegations have been confirmed by police investigation.

IDX has been stepping up efforts to improve its surveillance system after being hit by a series of frauds in the capital market in recent months, causing big financial losses to the investing public and tarnishing the credibility of the stock market authorities.

The latest case involves one of Indonesia's largest securities companies, PT Sarijaya Permana Sekuritas, whose president commissioner Herman Ramli allegedly embezzled investor funds worth Rp 245 billion (\$24.1 million). Herman is now in custody and the police are investigating the case.

An earlier and bigger fraud involves PT Antaboga Delta Sekuritas, whose owner also swindled customers' funds amounting to at least Rp 1.4 trillion. Both cases - in which the culprits amassed their ill-gotten money over several years - had prompted serious questions over the capital market authorities' ability and capability to monitor and detect possible investment frauds as soon as they occur.

Ponzi fraudster pleads guilty

A fund manager pleaded guilty last month to operating a \$80 million Ponzi scheme. Joseph S Forte faces up to 80 years in jail when he is sentenced for wire, mail and bank fraud, and money laundering.

Forte lured nearly 80 investors by promising impressive returns ranging from 18% to 38% and pledging they would suffer no losses. He used his Ponzi scheme to collect roughly \$80 million from investors, paying some 'returns' on their investments using money contributed by other investors. He also claimed he was profitably trading in S&P 500 stock index futures contracts through a partnership named Joseph Forte LP.

Instead he paid himself millions.

Forte consistently claimed that his trades were profitable, reporting fabricated investment returns. Despite the actual losses, he was able to continue raising money from new investors by falsely reporting high return rates. His method was two-fold: On a quarterly basis, he sent to an accountant email messages containing false representations about his trading activity, the status of the investors' investments and the worth of the partnership. At Forte's instructions, the accountant then sent the investors, via US mail, quarterly investment statements that were created based on Forte's misrepresentations.

Fraudster pays a high price

A convicted investment fraudster will serve 15 years in prison and has to pay more than \$6.2 million in restitution to the people he convinced to invest in his bogus companies.

Duane C Boechler, 52, was sentenced last month following his earlier conviction for scheming to defraud people of the money they invested with his companies from 1998 through 2007. A licensed securities agent until 1999, Boechler started a number of businesses - including Affiliated Valuables, Affiliated Homestead and Affiliated Natural Resources - and convinced people to invest \$7.6 million in the companies.

He helped his victims take out loans to invest with him, often using their houses as collateral; he induced them to sell other investments and cash out retirement accounts. Boechler gave at least six people mortgages on property he owned, each believing they had the only mortgage. And whilst he made some interest payments to his investors, he never repaid the principal in full, using the investments for his personal benefit instead.

Diary Date

2009 Malta International Financial Crime Forum

11-12 November 2009 at the Hilton Hotel, Malta. Euro 900.

Highlighting and examining the current issues affecting financial fraud, due diligence and financial intelligence. Hosted by the ICC Financial Investigation Bureau, Malta Financial Services Authority and the Malta Financial Intelligence Analysis Unit.

See www.icc-ccs.org/2009Malta

New corporate fraud may be South Africa's 'Madoff'

HUNDREDS of investors may have lost up to 10 billion rand (\$1.2 billion) in what could be South Africa's biggest corporate fraud.

Media reports last month alleged that Barry Tannenbaum, a South African businessman now living in Australia, lured around 400 investors over four years with the promise of 200% annual returns linked to pharmaceutical imports, and forged AIDS drug orders to reassure investors when money started to dry up.

The full extent of the scheme is still unclear, but lawyers and investigators believe hundreds of investors including top businessmen from South Africa, the United States, Germany and Australia, were involved, and that it could turn out to be South Africa's biggest corporate fraud. Tannenbaum was apparently well-liked and had a

'sterling' reputation in Johannesburg's elite business circles. Business colleagues describe him as unassuming and friendly.

But Investigator Specialised Services Group (SSG), a private law enforcement agency hired by investors to look into Tannenbaum, said he told investors they were funding a pharmaceutical ingredient import business.

Tannenbaum operated through his Frankel International and Frankel Chemical Corp. companies, and states in brochures that his father was a founder of South Africa's No 2 pharmaceuticals firm Adcock Ingram. Actually it was his grandfather.

Documents posted on the Internet by SSG include what they say are forged purchase orders from Africa's biggest generic drug maker, Aspen,

which Tannenbaum allegedly used to show investors that funds were coming soon. Aspen has confirmed that it bought small amounts of supplies from Frankel, but said the purchase documents, including some involving life-prolonging anti-retroviral AIDS drugs, were fake. In April, the money suddenly stopped, and investors tried to recover their cash.

The fraud has been likened to that of Bernard Madoff, with observers suggesting that Tannenbaum started legitimately. And like Madoff, it appears his scheme collapsed when investors demanded to be paid and new funds could not be found. No one knows where the money is at the moment.

Confronted by reporters at his office in Australia, Tannenbaum denied the allegations and refuted claims that he operated a Ponzi fraud.

OAPs on run from Iraq fraud investigation

AN elderly UK couple alleged to be at the centre of an international fraud investigation linked to a ghost arms scam involving the reconstruction of war torn Iraq have gone on the run.

American prosecutors say the couple, who run Zeroline from their home in Belton, near Yarmouth, took part in the large scale fraud after the fall of Saddam Hussein. When caught, Peter and Heather Tarrant, both in their 60s, could be hauled before American courts over allegations that \$8.5m in fake shipping bills were created for military hardware that was never delivered.

The alleged Zeroline fraud is one of about 80 investigations that the US has launched into potential waste and frauds from the billion dollar reconstruction of Iraq. According to Companies House, Zeroline is a private company limited by shares and as of March 31, 2008 had total assets, less current liabilities, of

£135,458. Mrs Tarrant is described as its company secretary/director and her husband is listed as an engineer.

During the chaotic aftermath of the war Zeroline was somehow awarded a contract to supply 51 armoured vehicles to Iraq's Interior Ministry in June 2004. The vehicles were never delivered to Iraq and the contract was ripped up in December 2005 by US authorities, but not before \$8.5m had been paid for their delivery six months before.

The fraud allegations against the Tarrant's surfaced after Massachusetts businessman Benjamin Kafka admitted his role in the \$8.5m fraud in April and agreed to cooperate with prosecutors. Kafka worked for the American branch of Alchemie Technology Group, a London-based firm to which Zeroline subcontracted the building and delivery of the armoured vehicles.

Legal papers claim that Zeroline and Alchemie presented false documents to JPMorgan Chase bank in London in June 2005, claiming payment for the vehicles - despite the machines never being delivered. The fake documents are said to a bill of lading made out to a fictional company GNX Logistics. Prosecutors allege that Kafka knew and permitted others to create a false bill of lading indicating shipment and receipt of the vehicles on a business form of a non-existent entity called GNX.

US fraud up

THE US Securities and Exchange Commission said in June that it has opened nearly 300 cases of suspected securities fraud so far this year, up 32% from last year. And the agency has already obtained emergency orders to freeze the assets of about 30 fraud suspects, compared with only seven at this point a year ago.

FIB members step up requests for due diligence checks

GROWING recognition about the importance of due diligence in the present economic climate has sparked a rise in enquiries from ICC Financial Investigation Bureau (FIB) members keen to know more about some of the people approaching them, and/or their assets.

The FIB says it has been offering a due diligence checking service for a while, but it is only recently that this has begun to vie with document investigations in popularity. It appears banks want to know more about the people they may be doing business with ahead of any transaction, says FIB Divisional Director John Lavers. They rarely tell us why, so we don't know in many instances if they are suspicious of a particular person or are just conducting due diligence as a matter of course and as part of good business practice.

Mr Lavers says that many of the due diligence investigations conducted by his staff do not reveal cause for concern, but occasionally they detect suspicious activity and, in a minority of cases, clear evidence of fraudulent intent. Nevertheless, the background information collected from a number of diverse sources can be very useful for future comparison if, for example, a person's business profile or lifestyle were to suddenly change, perhaps indicating involvement with or pressure from organised crime.

Evaluating risk

Outlining the nature of its work, the FIB says it is frequently asked to examine the relationship between two people and their individual or combined links to others, possibly high profile political people. Its checks include the individual's social/personal/business connections, together with any specified link the member is interested in. A confidential report is prepared that also includes its conclusions and, when appropriate, any advice regarding further contact.

This may include, for example, its advice in a recent enquiry that the subject posed a high risk based on the fact that he had direct access to politically exposed persons and that his father had been linked to criminal activities in the past. The client wanted to know if the son had any criminal links to his father, if he had any business links with his father's companies and what, if any, influence the father might be exerting over his son.

FIB investigators were able to discover that in the course of his work for a bank the son had daily contact with one of his father's accomplices. The accomplice was linked to the father's criminal activity, but there appeared no evidence of a criminal link between the son and his father's accomplice. Further enquiries did discover that the son was present on at least one occasion when his father kidnapped a prominent

banker, and that the son had refused to testify against his father at his subsequent trial. There was also evidence of shared company or business interests, and of the son's political contacts within the government of the country where he resides.

"This is just one example of the type of information we are asked to find out. In fact, requests for our due diligence checks are varied, but whatever they are we have a number of difference sources and methods that we use to ensure the reports are as comprehensive and accurate as possible," says Mr Lavers.

Similar techniques are also employed when the FIB is asked by members to investigate people who provide proof of funds that are set against assets they say they own. Recently, for example, a person said his company had sold the exploratory rights for oil & gas development that it claimed to own off the coast of West Africa, but the documents he provided as proof of ownership were insufficient on their own to confirm this. Investigators discovered it was extremely unlikely the man could have procured or sold the assets in the way he claimed and, after examining the business practice of the country concerned, concluded it was highly likely he obtained them using fraud, corruption or bribery. It therefore suggested that further investigations were needed to confirm the source and actual whereabouts of the funds, and that the applicant be asked to provide further documentation to support his claim.

Whilst detailed due diligence reports of the type outlined above take time to compile and often attract additional cost, the FIB reminds members that its standard checking service, provided within their membership package, can often reveal sufficient information to warrant caution and may be enough to resolve their concerns. For example, it says a recent enquiry involving a loan secured by a Bank Guarantee for a project in South Africa quickly revealed that two of those involved and their company had previously been reported to the FIB for involvement in a suspicious Bank Guarantee in 2008. Added to this was the fact that the document submitted contained enough 'red flags' and anomalies to make it highly suspicious in its own right.

"Given this information, revealed only after a superficial check, there was more than enough evidence to alert the member to be careful, and I'm sure they will not be taking this business any further," says Lavers.

"The point is that whatever the degree of detail, our approach and methods can help produce the most relevant and useful due diligence a member requires at less cost and in a shorter timescale than they could undertake in house," he adds.

Piracy's winners and losers explained

*Some of the anomalies in the current Somali piracy problem are illustrated in a series of articles published last month that help to clarify the winners and losers, and present another perspective on the situation. **Andy Holder** reports.*

The media has been quick, and quite right, to vilify piracy and bang the drum for action. After a slow start, governments caught the mood and sent naval ships to diffuse the situation. Their actions were further boosted last month in Rome when G8 ministers agreed the need for a common strategy to deal with piracy and highlight the jurisdiction problems that sometimes result in the release of captured pirates. At their meeting, the G8 ministers cited the need to strengthen their ability to investigate and prosecute piracy, in addition to recovering assets illegally obtained by pirates.

And in another move last month NATO defence ministers backed a plan for a long-term NATO anti-piracy mission off Somalia after the current operation ends. NATO Secretary-General Jaap de Hoop Scheffer said a British-commanded task force involving six NATO nations would take over the mission from July 1 for another 12 months, whilst other nations have indicated they may join the new mission in the future.

All good so far then, but their words must have seemed particularly poignant a few days later when nearly a dozen pirates captured by **HMS Portland** in the Gulf of Aden had to be released because they were not actually caught in the act or on the point of launching an attack.

Forces farce

HMS Portland is one of many ships serving with the Combined Maritime Forces Task Force 151, a multinational naval group that currently consists of vessels from the United States, Britain, Turkey, South Korea, Singapore, Denmark and Japan. It was established to conduct counter-piracy operations and has largely been deemed a success.

According to the report of the incident, **HMS Portland** detected two skiffs on its radar that it suspected were not innocent fishing vessels. The frigate steamed closer to the skiffs and saw that both vessels were filled with weaponry and ammunition. The ship's Lynx helicopter was sent to hover over the skiffs while teams of Royal Marine and Navy personnel in rigid inflatable boats sped towards the craft and disarmed the ten men on board (see photos below). Officials noted the skiffs were equipped with extra barrels of fuel, grappling hooks and a cache of weapons that included rocket-propelled grenades, machineguns and ammunition.

Despite this overwhelming evidence of their intent, the ship set the pirates free, though not before it confiscated their weapons and put all the pirates into one of the skiffs with enough fuel to get them to the Somali coast and told them to go home. The other skiff was then set on fire.

Explaining the action, a UK Ministry of Defence official said "Because of the rules of engagement, we can only arrest suspected pirates if we catch them in the act or on the point of launching an attack on a vessel."

Royal Marine and Navy personnel from HMS Portland approach and board two suspected pirate skiffs in the Gulf of Aden.



Piracy

“Clearly, with all the weaponry in the skiffs, there was intent to commit piracy, but we hadn’t actually caught them in the middle of an attack so had to release them. We basically removed or destroyed all the piracy paraphernalia,” he added.

A pirate’s experience

Nothing else is apparently known about the released pirates. They might go home, as advised, or they might return to try again. The chances are that they are not too dissimilar to the people profiled by Christian Science Monitor in a recent article, which describes how nine men got into their small, wooden boat one morning and left their village to seek their fortune in the Gulf of Aden. Their goal, shared by a Somali businessman living abroad who funded their weapons and boat, was to attack commercial ships and hold them for ransom.

Among them was Hassan Abdullahi, a fisherman with no seafaring experience who had never before worked as a pirate. Yet all nine leaving Bossasso were going to make their way west 250 miles along the Somali coast before turning north towards Yemen, where the busy shipping lanes narrow near the entrance to the Red Sea. The motive was money and their plan was to attack the first ship they came across.

Hassan, says the article, is the lowest rung in a criminal network that includes corrupt port officials, politicians, and investors from Europe, Asia, and America. The big money – with the average ransom now estimated at \$2 million, and ransoms paid said to total \$80 million last year – never reach people like Hassan, say Somali piracy experts. At most, mere gunmen stand to earn \$10,000 to \$20,000 apiece. But in a country devastated by two decades of war, where the average income is \$500 a year and 60,000 people are at immediate risk of starvation, \$20,000 for a little dangerous work is a risk worth taking.

Aged 20, Hassan told the magazine he decided to give piracy a try after seeing friends getting rich. But his first (and only) attempt didn’t go well. Having given themselves away by buying provisions from locals and asking advice on the best course to plot to Yemen, they were sitting ducks for one of the three patrol vessels operated by the independent republic of Somaliland coast guard. Having been tipped off by villagers, it knew where to find them and all nine were quickly captured in the ensuing fight. Back in Berbera’s central jail all admitted their criminal intent to attack ships, and six days later Hassan and the others were all jailed for 20 years for violating the

waters of a country they didn’t even know existed.

Hassan and his colleagues clearly paid a high price for their inexperience, but they were perhaps more fortunate than some other pirates that had earlier set off to attack a ‘merchant’ ship sailing near the Seychelles. It turned out to be the French naval ship **Nivose**. When it

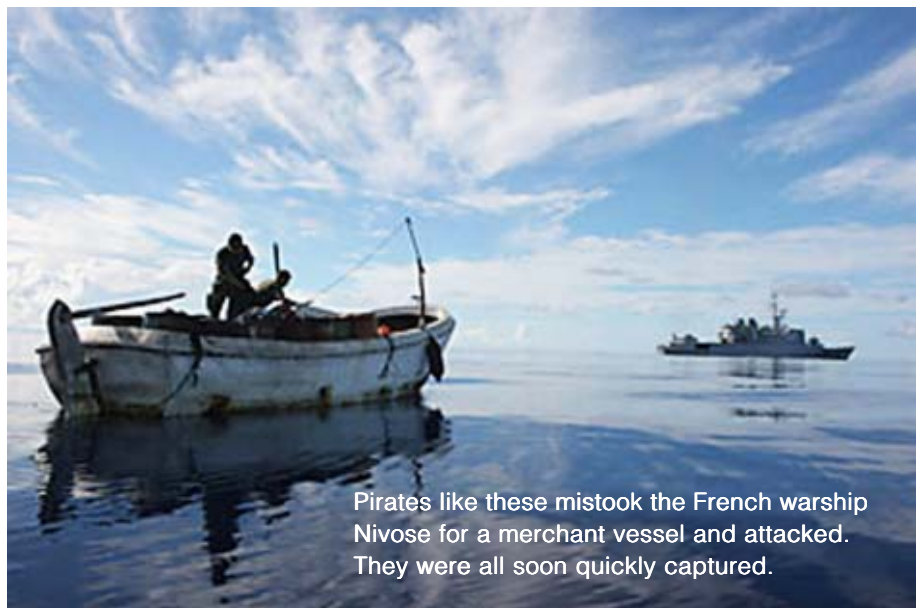
spotted the attack the **Nivose** headed into the sun to camouflage its identity before turning to confront the attackers whilst launching two boats and a helicopter. The helicopter fired warning shots and within minutes all 11 pirates in the three boats surrendered. Some were as young as 17.

Attacks down

The action taken by **HMS Portland** and the **Nivose** is evidence that the naval presence is having an effect, however, and the piracy monitoring agency the International Maritime Bureau (IMB) notes that the number of successful ship hijackings in the region is down significantly in recent months. Only one in 11 attacks in May was successful says the IMB. Moreover, there have been no hijackings in the Indian Ocean since May 2, and in the Gulf of Aden there were no successful hijackings between May 7 and June 11. And whilst pirates continue their operations in the region, it is notable they are now attacking more at night, it adds.



Hassan Abdullahi



Pirates like these mistook the French warship **Nivose** for a merchant vessel and attacked. They were all soon quickly captured.

Capturing the real villains

Unfortunately, say observers, capturing men like Hassan does as much to solve piracy as arresting a drug dealer does to win the war on drugs. The public face of Somali piracy may look like Hassan, but behind him is a vast network of investors and corrupt officials who buy the speedboats, weaponry, and GPS devices; who select targets from the Lloyd's of London list of insured ships; and who distribute the bulk of the dividends among themselves using underground money transfer systems.

J Peter Pham, an expert on Somali pirate financing compares it to an IPO (initial public offering). "For a start-up operation, you need more money, between \$150,000 and \$250,000, but if you want to provide capital to an existing operation, then you can give \$50,000 to have a share in the profits," he said recently.

Some pirate crews are given satellite phones to get real-time intelligence on the location and crew of a target. Some rent out "mother ships" to carry them far out to sea. Many of today's successful pirates track ships from port to port, often relying on inside information. The British newspaper The Guardian has reported that pirates have "consultants" in the close-knit ship-brokerage and insurance industries of London to help target ships. But shipping schedules are easily obtainable on the Web and in the local business press. Seeking ransom, the pirates are more interested in the crew than the cargo, Pham says.

The average ransom has risen sharply from \$1 million to \$2 million in the past six months. "Generally, roughly 30% of the ransom goes to the investors, 20% goes to the government officials and port officials or even Islamists who guard the boat while negotiations are going on," says Pham, who has interviewed former hijackers and knowledgeable Somali and Puntland

government officials. The remaining 50% goes to the pirates themselves, often paid out on the deck of the hijacked ship.

Big winners

The big players invest their money well, it is alleged. They buy property and, with a good accountant, launder their money in a stable third country such as Kenya, the United Arab Emirates or South Africa. Indeed, pirate ransom money is believed to account for the sudden influx of money in the Somali refugee enclave of Eastleigh in Nairobi. Ibrahim Ali Abdullah, a prominent Somali businessman there, says that while most streets in Eastleigh remain unpaved, gleaming glass-and-steel structures offering imported electronics and clothing at bargain prices are sprouting up.

Another beneficiary of the current situation is reported to be London's shipping insurers, because as the frequency of attacks rises, so, too, does their coverage of vessels plying pirate-infested waters.

Lloyd's of London syndicates make money insuring ships routed through the Gulf of Aden - US insurers do not cover piracy. Figures released recently by marine broker Aon reveal the surcharge for separate kidnap and ransom coverage could mean a shipowner pays an extra \$30,000 per journey - for every \$3 million worth of coverage - through high-risk seas - 10 times that charged last year.

With 22,000 Gulf transits a year, additional premiums could be worth up to \$400 million, notes Pham. Piracy, which for decades has been deemed 'low risk' and designated a 'marine peril', is now a 'war risk' that demands more expensive coverage. There are also additional protection and indemnity premiums covering crew safety - an issue of increasing importance as shipowners weigh the risks of hiring armed guards.



Forces close in on a vessel believed to be a pirate mother ship.

One shipping broker for a leading market player says his firm is surcharging a minimum of 0.125% of the hull value, rising to 0.2 at the top. War policies without the amended piracy clause cost around 0.025% early last year.

"Piracy does provide opportunities for some underwriters and premiums are higher," concedes Neil Smith, senior manager of underwriters at the Lloyd's Market Association, which represents the shipping industry. "But there's a very real risk of a total loss on the insurers' side when you have pirates operating with machine guns and RPGs."

Mr Smith urges caution in quantifying the profit from piracy, as premiums change on an almost daily basis, keeping pace with the risk.

“The Security/Privacy Paradox” – getting it right!

Privacy is considered a human right in Europe and to this extent organisations have focused on protecting the privacy of their customers' data. However, there's a blurring of lines between monitoring employee's activities to make sure that the organisation is secure, with the employees perception of a 'right to privacy.' In this article, **Adam Bosnian**, VP of Products, Strategy & Sales at Cyber-Ark shows organisations how to balance the security need to monitor employee activities whilst respecting their right to privacy.

To ensure the security of personal data, organisations have grasped the need to manage the people within the organisation by restricting the data they have access to, specifically, providing access only to the information needed to complete their specific business related activities. While this 'controlled' access is in line with the fundamental security tenet of 'Least Privilege', in order to ensure the integrity of its information, an organisation also needs to be able to identify if someone has done anything that they shouldn't have done with this information, or the underlying systems. For this reason companies need to know **1)** who is logging in to the system, **2)** what they're doing and **3)** if they had the right and approval to do so. This is managed in order to deliver another fundamental security tenet 'Trust, but Verify', so that the organisation can justify the activity based on the final piece of the puzzle – the captured and recorded activity log.

The actual identity of the users requiring access to key information is a vital element of robust, secure process. To that end, it is important to note that with many 'privileged' accounts within an organisation, there is no named, specific user. Instead, with these powerful, built-in accounts found in all applications, systems, operating systems, databases et al, the risk of a generic 'system administrator' account - designed to be used by many people without specifically recording the actual identity of any of them, is evident. In this case, a secure company must have a way of knowing who is behind a generic identity and collect subsequent activities in the same way.

An integral part of an effective corporate governance regime includes provisions for civil or criminal prosecution of individuals who conduct unethical or illegal acts in the name of the enterprise. It is therefore elementary that organisations must monitor and record employees conduct, compiling an audit trail that proves compliance with policies and takes preventative measures for data breaches. As the value in collecting the data is for the purpose of identification, only knowing that someone is accessing, changing or removing valuable information isn't enough. Organisations need to be able to pinpoint the individual, the associated activity, and whether this activity is in line with policy.

Do employees have a right to privacy?

Historically organisations in the UK have fallen foul of

the Data Protection Act (DPA) for failing to adequately protect customers' information – and this is replicated across the globe. However, even taking the security requirements and practices discussed previously, employees also have a right to the same protection for any identifiable data that is collected as part of audit trails and governance compliance.

Privacy concerns exist wherever personally identifiable information is collected and stored - in digital form or otherwise. Globally there are a number of different legislations that affect the way data is stored and used. The US has deployed a variety of different laws and regulations at both the national and state level that seek to provide consumer protection in a number of sectors where privacy issues have emerged. Examples include HIPAA, which addresses the requirement for healthcare providers and payers to keep Personal Health Information (PHI) secure and private, as well as other legislation requiring the credit card and financial services industry to also protect customers' non-public personal data and financial information such as the Payment Card Industry (PCI) standards and Gramm-Leach-Bliley Act (GLBA).

However, many uses of data fall outside the scope of this existing regulatory structure, and as such, are less strictly regulated. In Europe, The European Union Data Protection Directive (EU DPD) defines fundamental principles for privacy protection and includes mechanisms for cross-border transfers of personal data. Essentially, all principles are similar to the DPA in the UK that states anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- ✓ Fairly and lawfully processed
- ✓ Processed for limited purposes
- ✓ Adequate, relevant and not excessive
- ✓ Accurate and up to date
- ✓ Not kept for longer than is necessary
- ✓ Processed in line with your rights
- ✓ Secure
- ✓ Not transferred to other countries without adequate protection

Can we watch them?

It's important that concerns over privacy do not deflect from the strong case for monitoring employees' behaviour. Carsten Casper, Research Director with Gartner,

believes, "Security and privacy are not, and should not be seen as, mutually exclusive or opposing concepts. Modern legal and technical tools allow a balanced consideration of both."

Here are guidelines to avoid breaching privacy rights whilst gaining employee support:

1. Put policies in place explaining what is acceptable versus improper activity and/or behaviour – if you don't tell them how can they be expected to know?
2. Educate employees about what's expected from them and why it's important, to gain their appreciation and support for these important security measures and processes. Many employees may not even realise that their activities can cause a security breach.
3. Inform them that you can, and will monitor them and explain why
 - a. It is important that employees understand this works in their interests too as, if there is unacceptable or illegal activity, through monitoring it will be easy to identify the offender. This eliminates the finger of suspicion and the ill-feeling it can cause for those not involved and doing the roles in line with company policies. If they're not doing anything wrong they have nothing to fear!
 - b. Employees should be aware that personal activities during company time and/or using company products will also be monitored and recorded so there are no surprises.
4. Capture relevant information. When choosing a solution make sure that what it will capture is accurate, relevant and is kept secure from prying eyes
5. Recognise that an employee has a right to know what information you have, and be able and willing to access and share it with them

Carsten concludes, "Enterprises and individuals should not be forced to achieve security at the expense of privacy, or vice versa." Introducing a full lifecycle solution to secure, manage, log and monitor all privileged activity benefits all, whether it be with privileged information, privileged users or privileged processes.

With this type of full security solution in place, an employee is comforted by the knowledge that their employer knows they are doing their job in line with corporate governance and security policies. The employer is meanwhile reassured by the evidence that proves his employees are doing, and seeing, only what they are supposed to. And customers know they can trust the organisation to protect their personal information. Rather than allowing security and privacy to be at odds, following these steps will allow organisations to reduce the security risk whilst mitigating any privacy issues.

Insider snooping - from page 12

Type of Information	2009	2008
Customer Database	47%	35%
Email Server Admin Account	47%	13%
M&A Plans	47%	7%
Copy of R&D Plans	46%	13%
CEO's Password	46%	11%
Financial Reports	46%	11%
Privileged Password List	42%	31%

Ominously, 1 in 5 companies admitted having experienced cases of insider sabotage or IT security fraud. Of those companies, 36% suspect that their competitors have received their company's highly sensitive information or intellectual property.

Privileged Account Controls ineffective

Organisations are increasingly aware of the need to monitor privileged account access and activity, says the survey, with 71% of respondents indicating that privileged accounts are partially monitored, while 91% of those who are monitored admitted they are "okay with their employer's monitoring activities." Despite these efforts, 74% of respondents revealed that even with the controls being put in place to monitor them, they could still get around them, making current controls ineffectual.

Highlighting the ineffectiveness of current controls and access policies, 35% of IT administrators admitted they were using their administration rights to snoop around the network to access confidential or sensitive information. The most common areas respondents indicated they access are HR records, followed by customer databases, M&A plans, redundancy lists and lastly, marketing information.

"This survey shows that while most employees claim that access to privileged accounts is currently monitored and an overwhelming majority support additional monitoring practices, employee snooping on sensitive information continues unabated," says Cyber-Ark.

"Businesses must wake up and realise that trust is not a security policy; they have an organisational responsibility to lock down sensitive data and systems, while monitoring all activity even when legitimate access is granted," the company added.

The full report can be found at <http://www.cyber-ark.com/landing-pages/downloads/snooping-survey-2009.asp>.

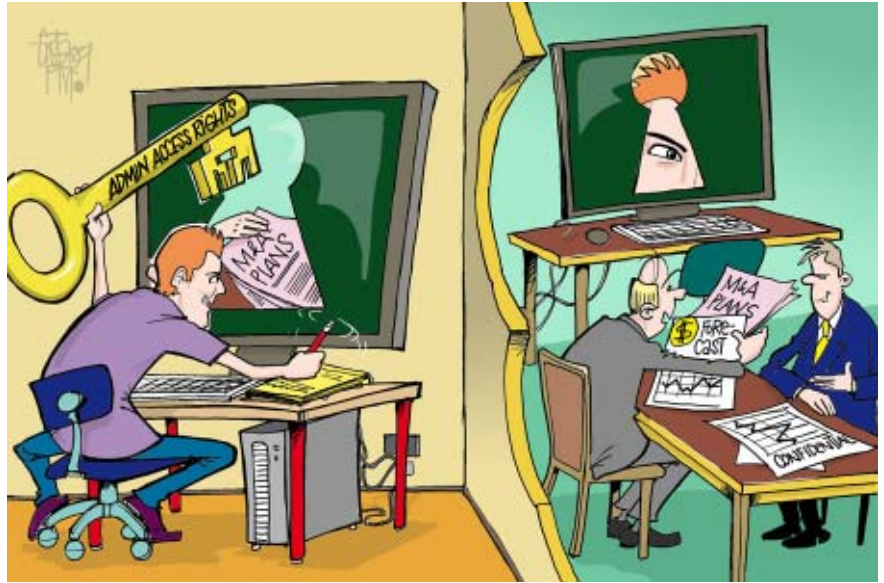


Corporate Security

Insider snooping on the rise

More than a third of IT staff admit to abusing administration rights to look at confidential information and 74% say they are able to get around controls designed to protect sensitive data. The figures are contained in the latest 'Trust, Security & Passwords' survey compiled by Cyber-Ark of more than 400 senior IT professionals in the US and UK.

Noting an escalation in the situation since last year, and despite the increased awareness that has followed numerous reports of data breaches, Cyber-Ark says that one of the most revealing aspects of the survey was the types and quantity of information employees would take with them if they were fired. As the



economic climate has worsened, the survey found a sharp increase in the number of respondents who say they would take proprietary data and information that is critical to maintaining competitive advantage and corporate security. When asked "What would you take with you," the survey found a six-fold increase in staff who said they would take financial reports or merger and acquisition plans, and a four-fold increase in those who would

take CEO passwords and research and development plans. Of the information targeted, respondents indicated they would be most likely to steal the following types of information:

continued on page 11/



COMMERCIAL CRIME

International

Subscription Order Form

I would like to subscribe to Commercial Crime International.
I understand that I may cancel my subscription at any time and receive a refund of the unexpired portion.

£95/\$160

Name _____
Job Title _____ Organization _____
Address _____

Postcode _____ Country _____

Tel No _____ Fax No _____

E-mail _____

Nature of Business _____

Please charge my Mastercard/Visa/Delta Card

Card number _____

Expiry Date _____

Signature _____ Date _____

I enclose a cheque payable to Commercial Crime Services (drawn on a UK bank)

Please invoice me/my organisation at the address above

Please return the completed form to: Commercial Crime Services
Cinnabar Wharf, 26 Wapping High Street, London E1W 1NG, UK.
Telephone Hotline +44 (0) 20 7423 6960

Commercial Crime International is published monthly by Commercial Crime Services. Cinnabar Wharf, 26 Wapping High Street, London E1W 1NG, UK.
Tel: +44 (0) 20 7423 6960
Fax: +44 (0) 20 7423 6961
E-mail: ajholder@gmail.com
Website: www.icc-ccs.org
Editor: Andy Holder
Editorial Tel: +44 (0) 1903 877081

ISSN 1012-2710

No part of this publication may be reproduced, stored in a retrieval system, or translated in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior permission of the publishers.

While every effort has been made to check the information given in this publication, the authors, editors, and publishers cannot accept any responsibility for any loss or damage whatsoever arising out of, or caused by the use of, such information. Opinions expressed in Commercial Crime International are those of the individual authors and not necessarily those of the publisher.

Copyright 2009. All rights reserved.