THE INKERMAN GROUP

INKERMAN ECONOMIC CRIME REVIEW

FEBRUARY 2013

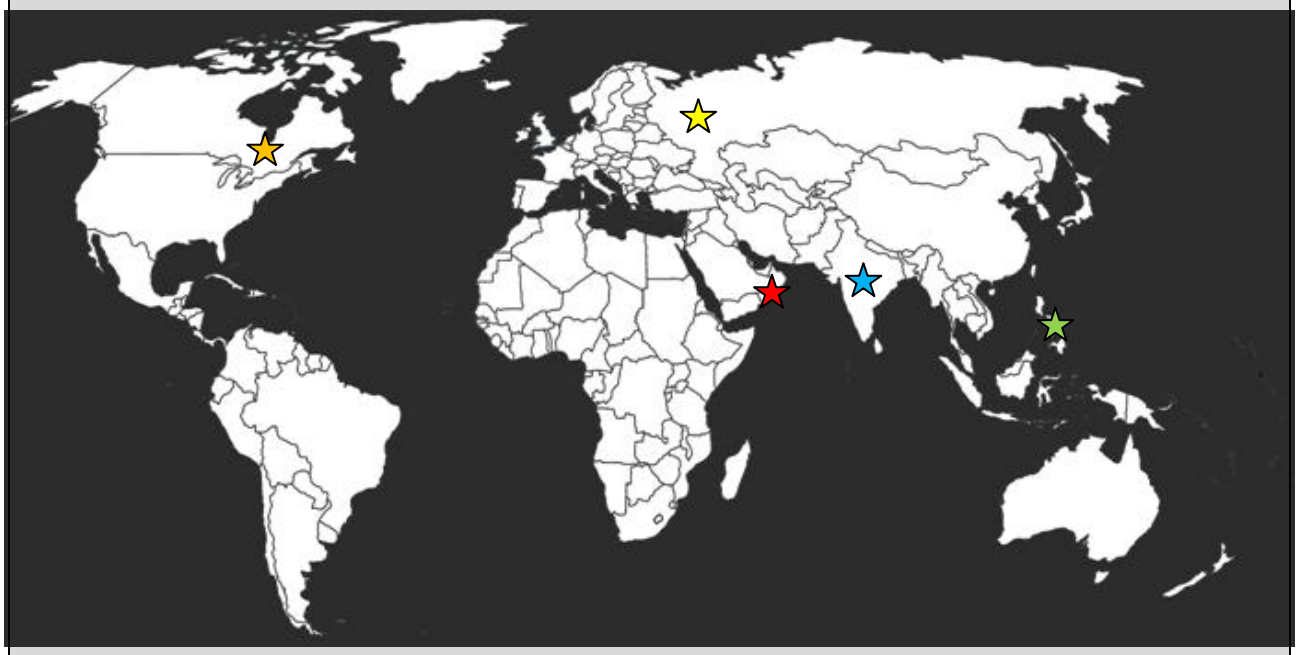
Companies operating in the modern business environment face an array of ever more sophisticated traditional and contemporary threats. These include: fraud, corruption, bribery, extortion, IP theft, counterfeit goods, cybercrime and scams. Keeping track of these prevailing operational risks is becoming an increasingly difficult, yet essential, part of both current and future operations. The Inkerman Economic Crime Review will give companies access to cutting-edge trend and incident analysis, which will enable them to ensure that prior prevention measures are in place or, if the worst should happen, contingency plans have been made.

INCIDENT WATCH

OMANI BANK HIT WITH CARD FRAUD *(PAGE 4)*

PROPOSALS TO STRENGTHEN ANTI-BRIBERY LEGISLATION *(PAGE 6)*

EFFORTS TO IMPROVE PROTECTION FOR HACKERS *(PAGE 9)*



FALLING VALUE OF COUNTERFEITS *(PAGE 10)*

UNCLEAR ACTIONS ON IP (*PAGE 12)*

FRAUD / CORRUPTION

BRIBERY / EXTORTION

COUNTERFEIT GOODS

IP THEFT

CYBERCRIME / SECURITY

TREND WATCH

In one of the most comprehensive annual reports into how fraud effects businesses across the globe, the '2012 / 2013 Kroll Global Fraud Report Survey', which is compiled by the Economist Intelligence Unit, has revealed some interesting trends with regard to fraud. The results are based on a survey of around 800 senior executives picked from a variety of industries, based in North America, Europe, Asia Pacific, Latin America, the Middle East and Africa. Whilst only a selection of the information can be reflected here, some of the most salient points include: insider fraud remains the biggest threat to businesses with 67% of all fraud cases committed by internal sources; the biggest concern to companies continues to be theft of information, which can occur due to targeted attacks or lack of employee care; perhaps most interestingly however, is that it appears that concern about fraud within business is falling faster than levels of fraud. With many commentators predicting that 2013 could be the year that both the UK Bribery Act and the Foreign and Corrupt Practices Act (FCPA) finally live up to the significant amount of hype and hyperbole surrounding their initial inceptions, there is evidence that this is a view which may also be shared by an increasing number of businesses. Evidence of this can be found in the discovery that the amount of organisations who have now conducted a through risk assessment of their current operations in light of the respective pieces of legislation has doubled in just over a year to 52%. Unsurprisingly, in terms of the most problematic regions in the world Africa continues to dominate, which despite seeing a general decline in the prevalence of fraud by 8%, levels remain worryingly high at 77%.

Perhaps in line with the finding in the above report that the biggest concern to the majority of business is the theft of information, the newly established National Alliance for Jobs and Innovation (NAJI) who describe themselves as "a nonpartisan organization of concerned businesses and industry experts working together to stop unfair competition from the use of stolen intellectual property (IP)" has announced its strategy to tackle IP theft. In particular, they have declared their intention to attempt to influence the government into introducing new policies and legislation that are specifically aimed at reducing piracy and IP theft. This, in turn, they hope will help to normalise competitiveness between American manufactures and those thought to be operating in high risk countries such as China and India. The creation of the NAIJ, which has seen well over 100 companies, including the National Association of Manufacturers and Microsoft combine their efforts to tackle IP theft, demonstrates the industry wide concerns about the potentially devastating costs of IP theft. This swell in interest is by no means just a US phenomenon however, and something that is likely to be in part driven by such global concerns was the announcement by the European Patent Office (EPO) that 2012 marked a record year in terms of patent filings. According to official figures the EPO received a total of 257,744 applications in 2012, although around 36.5% of these came from within Europe, it appears that much of the growth was actually driven by Asia, with China, Korea and Japan at the forefront.

Whilst by no means a new innovation, but something that does appear to growing increasingly prevalent, is this recognition across all forms of economic crime as to the benefit of all entities from small business, right up to entire nation states, taking a unified approach in order to help mitigate the risks posed by various forms of criminal activity. It appears that there have been a number of drivers behind this trend. The most influential is likely to be the fact that it does, on the whole, appear to be a successful strategy. This is demonstrated within this month's issue with a report stating that those countries which are a signatory to the Council of Europe Convention on Cybercrime experience levels of malware that are lower than would otherwise be expected. In addition, there is also increasing pressure

on large companies and government agencies to be open about security breaches and share information that could help prevent other organisations falling victim to similar attacks in the future.

FRAUD / CORRUPTION

SIGNIFICANT EVENTS

INDIA: EFFORTS MADE TO TACKLE CORPORATE FRAUD

In something of an ambitious project, India's Corporate Affairs Minister Sachin Pilot has outlined plans to develop a "foolproof" 'fraud protection model'. Clearly recognising the pervasive threat of high-level corporate fraud which has befallen India of late, Pilot hopes the model will give enforcement agencies the upper hand in early detection of suspicious money transactions and movements. In addition, the top official has recognised the need to strengthen the Market Research and Analysis Unit (MRAU), an organisation which he believes is "building capacity", but is currently unable to "detect fraud at an early stage to help prevent huge financial losses to people or the government". It is with this new model, therefore, that Pilot hopes to enhance the MRAU's capabilities, which although clearly an important step, its potential effects should not be overstated, something Pilot appears to have done when he declares that the changes will completely "insulate the economy from the disruptive effects of corporate fraud" within the next year, a claim that is likely to backfire.

UK: JOBSEEKERS UNWITTINGLY DUPED INTO MONEY LAUNDERING

Jobseekers and vulnerable low-income groups are being targeted by fraud gangs, according to reports from Financial Fraud Action UK (FFAUK). Criminals have been using job advertisements for "money transfer agents", "transaction specialists" and "payment processing agents" to recruit unknowing money mules to launder their ill-gotten gains. The scams aim to exploit those in need of extra cash by promising 'too good to be true' jobs, with the mule able to take a percentage of funds received into their accounts for simply transferring the rest to other, often overseas, accounts. Unbeknownst to the victim, the funds are usually the results of fraud and theft, leaving them open to criminal penalties as well as the closure of their bank accounts. Such mules are an indispensable part of the money laundering process, helping to disguise the money trail, and claiming ignorance may not be enough to avoid penalties. The scamsters have approached likely victims via mass emails and directly are identifying individuals from CVs posted to job seeking websites. Those identified as likely mules include students, new entrants to the UK and the unemployed. FFAUK has estimated that around 380,000 could have been affected by the scam.

OMAN: BANK MUSCAT HIT BY PRE-PAID CARD FRAUD

Oman's largest bank, Bank Muscat, has been hit by a US$39 million fraud involving pre-paid travel cards. Around twelve cards, which are used to allow travellers to carry foreign currencies without using debit / credit cards, were affected outside of the country on 20 February 2013, although none of the bank's customers were hit. Whilst investigations into the fraud are ongoing, it has been speculated that travel cards were duplicated, by manipulating the card database allegedly controlled by a firm in India, and then used several times in multiple locations. The day following the announcement saw a 4.3% drop in the bank's share price, the bank's greatest single-day stock fall since July 2011.

GLOBAL: FINANCIAL ACTION TASK FORCE UPDATE

Following their latest meeting held in Paris between 20 – 22 February 2013, the Financial Action Task Force (FATF) on money laundering (an intergovernmental organisation consisting of thirty-six members) has released the latest update. Of particular concern to the organisation are individual country's legal infrastructure in terms of providing an adequate base from which to fight money laundering and terrorism funding. There was positive news for Bolivia, Sri Lanka and Thailand, which have all now had their rating upgraded. In addition, Ghana and Venezuela are no longer to be subject to monitoring. The Philippines were given the rather direct instruction to update recently enacted anti-money laundering legislation so as to include casinos in the list of businesses that are required to report suspicious transactions to regulators. India were also praised for their so-called 'Aadhar' programme which the FATF have acknowledged "if successfully implemented, the Aadhar project would be the first biometrically verified unique ID implemented on a national scale and would provide the "identity infrastructure" for financial inclusion as well as for strengthening anti-money laundering and combating terrorist financing implementation. Meanwhile, Turkey narrowly missed being labelled a "high-risk or uncooperative jurisdiction" and suspension from the FATF, signing a bill to reduce the financing of terrorism just before the FAFTs deadline.

BRIBERY / EXTORTION

SIGNIFICANT EVENTS

ITALY / INDIA: FINMECCANICA KICKBACKS IN SPOTLIGHT

Bribery allegations involving defence firm Finmeccania and senior Indian officials has dominated headlines this month. The firm has been accused of using kickbacks to obtain a US$750 million contract with the Indian government for twelve Augusta Westland helicopters from Finmeccanica SpA in 2010. In documents leaked to the media, it is alleged that €100,000 (US$130,240) was paid to relatives of the head of the Indian Air Force from 2005 - 2007, Air Chief Marshal S.P. Tyagi, as well as other monies directed to the Northern League political party, and that allegations had been made by a manager that was subsequently fired. The allegations, which Finmeccania deny, resulted in the arrest of CEO and Chairman Giuseppe Ors on 12 February 2013 by Italian investigators after a two year investigation, leading to his resignation on 15 February 2013. The incoming CEO, Alessandro Pansa, instituted a board shakeup, including replacing the head of AugustaWestland. The scandal is embarrassing for the Indian government, who has been implicated in numerous corruption scandals in recent years, with opposition parties taking advantage of the situation. For its part, the Indian government has been keen to show a tough stance against the firm, cancelling the contract and ordering its own investigation by the Central Bureau of Investigation. It is likely that as the investigations continue, India will blacklist the Italian firm, reducing its source base for military contracts despite warnings from military analysts against the potential negative impact of any such move on the military.

LIBYA: INVESTIGATIONS INTO RELATIONSHIP BETWEEN GADDAFI AND GOLDMAN SACHS CONTINUE

Libyan Prime Minister Ali Zidan is still trying to make amends for Muammar Gaddafi's unscrupulous dealings with international firms, particularly those in the banking sector. In February 2013, representatives from the Libyan Investment Authority (LIA) confirmed that they are now working in conjunction with officials from the US Securities and Exchange Commission (SEC) to investigate the relationship between Gaddafi and Goldman Sachs Group Inc. The New York-based banking giant is believed to have violated American anti-corruption laws in mid-2011, by allegedly bribing Libyan government officials. Goldman Sachs, along with other banking companies, are believed to have sold the Gaddafi regime "complex investments" as means to hide some US$50 billion in assets. In 2008, the LIA reportedly lost 98% of its total worth, after engaging in complex deals with Goldman. In an attempt to recoup these losses, Goldman Sachs allegedly agreed to pay fee of US$50 million to the Gaddafi regime. According to the SEC, LIA attempted to transfer the fee to a third-party investment firm, Palladyne International Asset Management BV, which at the time was controlled by the son-in-law of the state-run National Oil Corporation (NOC).

CANADA: PROPOSALS TO STRENGTHEN ANTI-BRIBERY REGULATIONS

The Canadian government has signalled its tougher attitude towards foreign bribery by proposing amendments to the Corruption of Foreign Public Officials Act (CFPOA) in a bill introduced on 05 February 2013. The current proposals make considerable changes to the existing anti-bribery law, bringing it more in line with other western benchmarks, such as the

UK's Anti-Bribery Act and the US' Foreign Corrupt Practices Act (FCPA). The bill proposes to expand the jurisdiction of the CFPOA, as the current law only covers activity that has a "real and substantial connection to Canada", a considerable weak-point in any anti-bribery measures. However the proposal expands the law's jurisdiction to cover all activities of Canadian companies and citizens, and broadens the business dealings it covers to any business related activity, not just those for profit. It also sets out the long-term removal of exemption for facilitation payments (AKA grease payments) which are currently permitted. This move is more in-line with UK legislation which also prohibits facilitation payments (this are exempt under the FCPA) Additional plans include: making it an offence to falsify or conceal records related to bribery of a foreign official; providing exclusive CFPOA jurisdiction to the RCMP to prevent any conflicts between federal and provincial law; and toughen penalties by increasing the maximum length of imprisonment for individuals from the current five to fourteen years. Whilst the proposals are in their early stages, the amendments will have considerable impact on Canadian businesses operating abroad.

ALGERIA: SNC-LAVALIN BRIBERY SCANDAL ESCALATES

Last month Canadian-based construction firm, SNC-Lavalin, found itself in hot water over its alleged unsavoury dealings with yet another Maghreb government. On 21 February 2013, Canadian news outlets confirmed that the company was under investigation on suspicion of bribing Algerian authorities. The police inquiry appears to be centring around Farid Bedjaoui, the nephew of Algerian former affairs minister Mohammed Bedjaoui, who is believed to have acted as a go-between for SNC-Lavalin and other international firms by offering "suspicious payments, possibly bribes" to leaders in exchange for lucrative deals with Algeria's state-owned energy giant, Sonatrach. SNC-Lavalin, which saw a number of senior executives arrested in connection with fraud and money laundering deals with the Libyan government under Muammar Gaddafi, is not the only firm to have raised suspicion in Algeria. In November 2013, The Inkerman Group reported that Italian authorities were also investigating oil services giant Saipem – a subsidiary of Eni – over its questionable link to Sonatrach. As these cases show, those wishing to invest in Algeria are often faced with the threat of bribery, and foreign companies are often encouraged to 'grease the palms' of Algerian authorities. This is largely due to Algeria's traditionally vague hydrocarbon sector laws and extensive red tape, which make it difficult for international firms to make an honest footprint in the Maghreb nation.

CYBERCRIME / SECURITY

SIGNIFICANT EVENTS

USA: EXECUTIVE ORDER GETS THE BALL ROLLING

On 12 February 2013 the US released a Presidential Executive Order to kick start the US' cyber security legislation. President Obama was forced to issue the unclassified order after Congress failed to agree on cyber legislation in 2012 due to, amongst other things, concerns over civil liberties violations. The Order focused on measures to protect US critical infrastructure from cyber attacks and on information sharing. Federal agencies have been tasked with identifying critical infrastructure – organisations where a cyber attack could have a catastrophic regional and national impact – as well as producing a cyber security framework which incorporates "voluntary consensus standards and industry best practices to the fullest extent possible". Information sharing was also identified as a key risk mitigation strategy, with the order focusing on information sharing from government to the private sector (skirting around the more controversial topic of information flowing from private organisations to the government) and the increased use of private cyber experts. For these reasons, the Order has its critics, with a number arguing that it "lacks teeth". For example, Stroz Friedberg has argued that all companies need government-shared intelligence, not just critical infrastructure firms, and others have criticised the emphasis on voluntary minimal standards. It is a first-step in tackling the thorny issue of cyber security but it does not replace the need for comprehensive legislation.

UAE: DUBAI CYBER CRIME GANG ARRESTED

In a coup for authorities in Dubai, it was confirmed that members of a cybercrime gang thought to be behind the theft of US$1.9 million from companies listed on the Dubai Financial Market have been arrested. Dubai Police's Electronic Intelligence Team reportedly nabbed gang members of African and Asian origin who participated in the scam, seizing cash, forged cheques and luxury vehicles. The masterminds behind the fraud are thought to have hired professional hackers to launch cyber attacks against Dubai-based businesses, often infecting corporate systems with malware to gain access to electronic transfer statements. Once compromised, company accounts would be looted, with funds channelled through bank accounts belonging to fictitious companies. As is typical with internet crimes, the fraudsters are thought to be based in several countries, with Dubai police reporting that further suspects are thought to be operating in Africa.

LIBYA: LOCAL HACKING GROUPS IN THE SPOTLIGHT

There appears to be an emerging group of hackers with Libyan links, who are keen to infiltrate Libyan-related websites. Illustrating this, a hacker with the online screen name "QuisterTow" took credit for infiltrating the website of Benghazi-based oil giant, Arabian Gulf Oil Company (Agoco), on 06 March 2013. QuisterTow claims to have hacked into the main page by identifying a "critical" vulnerability to the website's Structured Query Language (SQL). It is believed that the user input in Agoco's website at http:// agoco.com.ly, may have been either incorrectly filtered for dangerous characters, making it more accessible to cyber attacks. As a result of the website's vulnerability, QuisterTow claims to have been able to access the Agoco's entire website database from the server, before

posting its login and password information on the website, Pastebin – a common tactic used by international hackers. The 'leak' by QuisterTow showed that the pass code used by the

DISCLAIMER

OPERATIONS CENTRE
INKERMAN HOUSE 3-4 ELWICK ROAD
ASHFORD KENT TN23 1PF

THE INKERMAN GROUP
1 CORNHILL
LONDON EC3V 3ND

THE INKERMAN GROUP
AM MEERKAMP 17-19
40667 MEERBUSCH
GERMANY

REG IN ENGLAND NO: 3085655
VAT REG NO: 787297952
CONSUMER CREDIT LICENCE NO: 420332
DATA PROTECTION: Z6511514

T + 44 (0) 1233 646940
F + 44 (0) 1233 646840

T + 44 (0) 20 7589 5338
F + 44 (0) 20 7589 5339

T + 49 (0) 2132 968 5151
F + 49 (0) 2132 967 9582

enquiries@inkerman.com
www.inkerman.com

