FORENSIC SERVICES

INTELLIGENT INTELLIGENCE

THE IMPORTANCE OF ORGANISATIONAL INTELLIGENCE TO THE MAKING OF GOOD QUALITY BUSINESS DECISIONS

JIM GEE,
PROFESSOR MARK BUTTON
AND STEVE KELLY

OCTOBER 2013
## CONTENTS

1. INTRODUCTION  
   1

2. ORGANISATIONAL INTELLIGENCE THROUGH THE AGES  
   2

3. THE LATEST TECHNIQUES  
   7

4. CONCLUSION  
   9

ABOUT THE AUTHORS  
   11

ABOUT THE PUBLISHING ORGANISATIONS  
   13
1 Introduction

1.1 This report highlights the importance of using good quality intelligence in the making of good quality decisions.

1.2 Over the centuries the circumstances in which it is just too risky not to make good quality decisions have lead governments and armies to develop and invest in intelligence gathering techniques. These have included decisions about military operations and national security and the techniques employed have got progressively more sophisticated.

1.3 Military intelligence has focussed on the capacity and intentions of enemy forces (i.e. the threat has been external) while intelligence intended to protect national security has focussed both externally (on opposing powers) as well as internally (on potential threats from within) – hence the existence of Secret Intelligence Service (MI6) with an external focus and Security Service (MI5) which is focussed internally.

1.4 Corporate intelligence gathering had also become the norm in the private sector as the end of the 20th century neared. It has normally focussed on understanding the market that a company is operating in or on competitors and their products and services. It is now also normal to gather information about potential new employees (pre-employment checking) or business partners (due diligence).

1.5 The historical trend can therefore be seen to be one where the importance of intelligence is being gradually recognised in a wider and wider range of decision-making contexts. However, with the digital age has come ever greater volumes of available data, and the challenge now is to extract the relevant information from that data and to make sense of it. This is no small challenge. Simply using the Google search engine can elicit information – often supporting both sides of a proposition – and the volume of information is impressive. Sadly, the quality of that information often is not.

1.6 The challenge arising from the reality that ‘more is less’ has been one of the drivers behind the more widespread use of intelligence analysis techniques that were formerly only deployed in a military or national security context. Some of the rogue operators whose bad practices have been highlighted in illegal phone-hacking and accessing unauthorised personal information have responded in the wrong way to this challenge.

1.7 Apart from the unethical and illegal nature of such work, it is actually not the most effective way to find out what is needed. With more and more information being digitised, the analysis of the patterns of data or what is called ‘data visualisation’, provides a professional, legal and ethical way of accessing good quality information.

1.8 This report sets the latest techniques in a historical context, and introduces the new (to the commercial sector) technique of Digital Communications Mapping. It seeks to cast to one side the techniques of the ‘film noir’ private detective, the stereotypical investigative journalist with the long lense camera and the cold war intelligence agent.

1.9 Intelligent intelligence in the business world means using the latest digital intelligence techniques to understand both the external context and the internal reality. Do communications flows within an organisation match what is intended according to the structures and processes which have been established? Are there undisclosed or inappropriate networks present? In the interactive world of the 21st century it is not enough just to make the right decision, it is also important to understand how to implement the right decision in a context where competing demands and motivations can make this difficult.

1.10 It is hoped that this report highlights how this can be achieved and in so doing makes its own contribution to better quality decision making and greater corporate integrity.

Jim Gee
Director of Counter Fraud Services, BDO LLP and Visiting Professor and Chair of the Centre for Counter Fraud Services at University of Portsmouth
2 ORGANISATIONAL INTELLIGENCE THROUGH THE AGES

2.1 The use of intelligence, both in the military and beyond, is nothing new. Due to the secretive nature of some of the work it is difficult to establish exact details of the intelligence techniques historically employed, but evidence of intelligence operations can be found in nearly every civilisation that has left historical records.

The Egyptians

2.2 According to Terry Crowdy, in his book The Enemy Within: A History of Espionage, “the earliest surviving record of espionage dates from the time of Pharaoh Rameses’ war with the Hittites and the Battle of Kadesh (c. 1274 BC). The Hittite king Muwatallis sent two spies into the Egyptian camp posing as deserters to convince the Pharaoh that the Hittite army was still quite distant. Rameses believed their story and unwittingly allowed part of his army to march into a Hittite ambush. Fortunately for the Pharaoh, he captured two more Hittite spies and had his officers interrogate them. The Hittites spies revealed that an ambush had been set and Rameses was therefore able to bring up reserves and avert disaster at what became known as the Battle of Kadesh”.

2.3 The veracity of the report itself is dubious in so far as the primary account of the battle is that of the Egyptians and therefore heavily biased. The idea that any advantage gained by the Hittite ruler was only by vile deception and that it was Rameses’ vigilance and cunning that saved the day seems all too convenient in historical context. True or not, the fact that at the time of writing it was seen as plausible that an information gathering mission and misinformation campaign could have taken place tells us something of their understanding of intelligence practices.

2.4 For it to be believable that the Egyptian camp was infiltrated and subsequently deceived, it can be inferred that the Egyptians had a similar capability and intent. For such a strategy to be possible, the military command will have needed access to specialists who were skilled at deception and who were trained to know what details would be important to bring back to the military command. Those specialists will need to have been identified, recruited for that purpose and managed in some capacity. They will have needed some kind of mechanism by which those in a position to coordinate a deception could also coordinate an ambush.

2.5 The Egyptian soldiers will have needed to be looking for spies for it to be believable that they may have detected them. The soldiers will likely have been briefed in some capacity to do so and will have needed to know the procedure for reporting such suspicious activity. Assuming that the 21 year old Pharaoh did not personally oversee all aspects of such matters, it can be inferred that at the very least the Egyptians had persons acting in the roles of modern day intelligence officers, if not a permanent posting to fulfil that function.

Sun Tzu

2.6 The further forward thorough history you go, the more descriptive and prolific the writings concerning intelligence matters become. Chapter 13 of Sun Tzu’s book ‘The Art of War’ (c. 500 BC) concerns itself exclusively with the correct use of spies. Although it talks about what spies should be used for and the sorts of things a ruler should have them do, it talks little about how that information should managed or how the intelligence network should be organised.

The Arthashastra

2.7 Another, somewhat less well known, book from the period relating to such matters is The Arthashastra. It is believed to have been written by Châllakya (c. 350–283 BC), who was a scholar at Takshashila and the teacher and guardian of Emperor Chandragupta Maurya, the founder of Mauryan Empire. The Arthashastra is an ancient Indian treatise on statecraft, economic policy and military strategy which talks about the usage of spies in both a military and commercial context. It is believed to be written as a pragmatic record of how a state is run, rather than an ideology for how a state should be run.
2.8 The Arthashastra goes into some detail as to how to set up an elaborate intelligence network. It suggests that with the aid of ministers, who have had their loyalty rigorously tested, multiple “institutes of espionage” should be created independently of one another. For any given mission three institutes may be given the same task. This would provide protection against single source reporting and help identify spies who are unreliable or corrupt.

2.9 The book states “When the information thus received from these three different sources is exactly of the same version, it shall be held reliable. If they (the three sources) frequently differ, the spies concerned shall either be punished in secret or dismissed”. The institutes themselves appear to have been run by a Master of the Spies who was to recruit spies of differing stations and, depending on their skill sets and social standing, to perform different functions. These functions included information gathering, sowing misinformation or dissent, subversion and assassination.

2.10 Unlike The Art of War, which generically states that you should “use your spies for every kind of business”, the Arthashastra talks specifically about “The Conduct of Corporations”. The definition of the term corporation in this context is somewhat different than that which we might understand today but still encompasses mercantile and agricultural organisations. The book states that to a ruler “The acquisition of the help of corporations is better than the acquisition of an army, a friend, or profits.” and that “Spies, gaining access to all these corporations and finding out jealousy, hatred and other causes of quarrel among them, should sow the seeds of a well-planned dissension among them”. It goes on to describe a number of other methods of control, from employing harlots “endowed with bewitching youth and beauty” to a well-placed assassination.

2.11 The importance of commercial support seems to have been as highly valued then as it is in politics today. Although the tactics used for regulating those corporations and winning their support would now be seen as somewhat underhanded, the principals of establishing a solid foundation of reliable intelligence before effective action may be taken were clearly understood.

2.12 Creating a personal intelligence network can be a lengthy and expensive process but was fundamental at a time when society was less well developed and reliable information was harder to come by. As civilisation became more developed there were increased opportunities for exploiting the resources already available. At around the same time as the Arthashastra was thought to be written the Romans were already a dominant force. This was despite having no postal communications system, no government intelligence service, no permanent foreign service and no decision-making body other than the cumbersome three hundred man Senate. Rome had prevailed against Hannibal in the Second Punic War but suffered heavy losses. This was largely down to Hannibal’s ability to take advantage of intelligence led opportunities due to his being his own principal intelligence officer and supreme commander of forces.

2.13 Part of Rome’s reluctance to develop a formal intelligence service stemmed from the way its republican government had developed. The Senate was comprised of a great number of different wealthy families with an equal number of differing personal objectives. They employed private intelligence networks of business associates, informers, clansmen, slaves or agents who could keep them informed of events at home and abroad. It would have been seen as too dangerous to create a single central intelligence organisation that might fall into the hands of a rival faction.

2.14 Caesar changed this when he was elected dictator in response to a civil war with Pompey (c. 50 BC). He established a rapid message and information transport system via couriers and routinely used counterintelligence techniques, such as codes and ciphers, to prevent his military plans from falling into the hands of the enemy. His successor, Augustus, had a better opportunity to develop the system that Caesar had created. Augustus established a state postal service called the Cursus Publicus, an extensive network of outposts which could provide fresh mounts and feed for couriers. The Cursus Publicus also acted as a freight service moving heavier goods throughout the empire.

2.15 As the system of the Cursus Publicus developed, the couriers were drawn increasingly from the army, especially from the Speculatores. Originally a scout and reconnaissance element of the Roman army, the Speculatores were recruited from the best riders of the Praetorian cavalry. The duties of the Speculatores were not limited simply to carrying messages. There role developed into one akin to a modern day security service, even acting as imperial bodyguard.
2.16 With Hadrian (c. 117-138), came another innovation that added more manpower to this intelligence network. Supply sergeants, called Frumentarii, whose original functions had included the purchase and distribution of grain, were recruited as intelligence officers. Because these men were constantly traveling on logistical assignments, they were in a position to watch over the army, the imperial bureaucracy, and the local population. The Frumentarii began to replace the Speculatori as intelligence couriers and eventually as secret police. The late empire came with a rise in levels of bureaucracy and an increasing number of government organisations performing intelligence functions leading to the Romans institutionalising its information services and espionage activities under the Master of Offices; who effectively acted as Minister of Information. It cannot be said that they ever established a formal intelligence service as we would know it today, but they came close.

Wellington, the Boer War and into the 20th century

2.17 For many years armies tended to form small ad hoc intelligence organisations during campaigns in order to provide the commander with the necessary military intelligence. Lord Wellington employed Exploring Officers and code breakers but, despite their success, the military intelligence organisations were disbanded in peacetime.

2.18 A variety of information and intelligence gathering units were raised during the Boer War 1899-1901, and due to the volumes of information obtained, there developed a need to analyse the information collected. This led to a three-tier system of sources and agencies employed to collect the information, field intelligence officers with the combat units and staff intelligence officers with the formation headquarters able to analyse the information.

2.19 By the end of the war the intelligence element of the British Forces increased from 2 officers to 132 officers and 2321 soldiers but again, at the war’s conclusion, the intelligence units were disbanded.
2 ORGANISATIONAL INTELLIGENCE THROUGH THE AGES

The creation of MI5 and the Great War

2.20 In 1909 a small counter intelligence department, later known as MI5, was established in anticipation of the Great War and by 1912 a second department, MI6 or the Special Intelligence Section, was established to control intelligence gathering overseas. Following the lessons learned in the Boer War, steps were taken to raise an Intelligence Corps at the outbreak of war in 1914. Former Metropolitan Police officers operated as field security police behind our own lines identifying enemy agents. The Field Security Police helped ensure that the rear areas and lines of communications remained free from the threat of subversion, espionage and sabotage.

2.21 Communications technology had moved on since the Boer War and although signals intelligence was a new military science, from the early months of the war the British were able to locate German units through simple direction finding. Many German signals were sent in clear at this stage as the need for radio cryptography had yet to be established. The Germans developed a system of tapping the vast network of landline communications employed by the British. The Allies only became aware of the eavesdropping equipment in early 1916 but succeeded in duplicating the apparatus. By the end of the war equipment had been developed to the extent that it was possible to monitor signals from a landline from 3000 yards away.

2.22 With the growing capability of powered flight, aircraft could now be used for reconnaissance, a task today often performed by unmanned drones. Kite balloons were also employed by the army to give a better view of the battlefield. In 1915 stereoscopic imagery was introduced giving depth to the images. Between July and September 1916 alone some 19000 photographs were taken of the Somme battlefield. By this time each squadron needed three intelligence operatives attached to interpret the huge quantities of photographs taken.

2.23 Despite the use of these new technologies, intelligence services still successfully employed spy networks not dissimilar to those described in ancient times. In Europe these were able to observe the movement of German troops across the continent and provide timely and accurate indications of German intentions. Although rebranded to the more palatable name of psychological operations, propaganda and the sowing of decent amongst the population remained effective weapons of war.
2.24 During the Second World War, signals intelligence made significant advances when compared to the simple tactical interception and direction finding of the First World War. Radio interception outposts became more prolific, and at the tactical level, mobile signals interception units provided technical surveillance capabilities close to the front.

2.25 The rapid increase in photography seen in the First World War was largely dealt with by increasing the number of people reviewing the available data. Signals data, whilst certainly growing by volume, was also growing in complexity. The codes and cyphers employed became increasingly more sophisticated, and due to the mathematical nature of the problem, the use of electromechanical machines by intelligence agencies for both encryption and code breaking was widespread. As the volume of data grew, intelligence agencies realized that a new tool would be needed to keep up.

2.26 In 1936, Alan Turing provided an influential paper intended to solve a mathematical decision-making problem posed by a prominent German mathematician. He proposed a hypothetical machine that would be capable of performing any conceivable mathematical computation if it were representable as an algorithm. Turing would later start his well-documented work at Bletchley Park where he would witness the creation of the first fully programmable digital computer.

2.27 The invention of the computer led to what would become known as the Information Age in which we now live. The world’s governments invested heavily in computing in an effort to get the technological edge. After the war, computing came to the commercial world, where the technology soon became big business.

2.28 Computers were getting faster exponentially. Gordon E. Moore, co-founder of Intel, noted in a 1965 paper that the number of components in integrated circuits had doubled every year from the invention of the integrated circuit in 1958 until 1965 and predicted that the trend would continue. This became known as Moore’s Law and is now used in the semiconductor industry to guide long-term planning and to set targets for research and development.

2.29 With the invention of the internet in 1969, the volume and methods of communication we use today have also increased. Today, every minute, hundreds of millions of phone calls and emails are sent, two hundred and seventy seven thousand people log into Facebook, over one hundred new LinkedIn accounts are created, three thousand photos are uploaded, and 2 million people Google something.

2.30 For those who work in the intelligence industry, the unprecedented volumes of data bring with it both challenges and opportunities. Volume data produces patterns and patterns can be used to predict future behavior, but these patterns can be difficult to find. The latest intelligent intelligence techniques identify and analyze these patterns.
3.1 One such technique used by today’s security forces is Digital Communications Mapping (DCM). DCM is a process in which a trained analyst models communications data so that it may be more easily analysed and understood. The analyst will import the data into a suite of specialist software to create a number of different visualisations and datasets. These visualisations will be analysed to identify areas of interest and any patterns that may emerge. Depending on the area of interest or pattern which is identified the analyst will, where possible, remodel the data to facilitate a deeper analysis. Once all reasonable avenues of investigation have been pursued, final conclusions will be drawn and an intelligence report will be produced.

3.2 The areas of interest that first need to be identified are the key nodes in the communications network. This is done by running mathematical algorithms over the data model to measure each node’s potential for influence and control over the rest of the network. This is based on its relative position to, and weight of communication with, all of the other nodes in the network. This can be done on an organisational or individual level depending on the intelligence requirement and the data available. The data model will then be analysed to identify if the key nodes and the nodes they communicate with fit with organisational expectations and to see if any patterns of interest emerge; anomalies will be further analysed where appropriate. Where possible, the analyst will look at the date and time of communications in sequence to identify temporal patterns and suspicious behaviour.

3.3 The necessity to understand this data has wider reaching implications than just those employed by security services. The communications boom has effected most organisations regardless of whether they are public or private sector. Historic organisational theory was built on the assumption that organisations are mechanical things, in which the parts (including employees functioning in defined roles) are interchangeable. It was taught that individual difference could be minimized or even eliminated with careful management techniques. In this way a robust communications strategy template could be successfully implemented across an organisation and effective decision making could take place.

3.4 The reality is that regardless of the robustness of a communications strategy, people will act within bounded rationality and are influenced by individual cognitive bias. Like the Ancient Roman senate, the majority of individuals will naturally act to meet personal objectives before considering the greater good. This does not mean there is no value in defining a communications strategy, or even that such a strategy does not work. It merely acknowledges that talented individuals will often work a system, with varying degrees of compliance, so that local objectives are achieved regardless of how well a strategy fits their needs.
3.5 By mapping the communication data, it is possible to see how a group of individuals communicate in practice by identifying the key nodes in the network that are controlling the flow of information and areas of the network where information should be flowing, but is not. With this information, measures may then be taken to improve the communication flow where it is lacking, capitalise on talent that may have been previously unidentified and redistribute control where it is seen to be inappropriate.

3.6 What is considered to be a key node depends on the network being considered and the objective of the analysis but will normally be the person that is best placed to control the flow of information. When one considers the complex spy networks of ancient times there was often necessity for one espionage network to spy on another to identify corruption. DCM then, would provide the modern day equivalent, identifying if the information flow met with organisational expectations or not so that action may be taken.

3.7 A network may fail this test for many reasons; decision makers often delegate responsibilities to competent subordinates moving the communication flow to unexpected areas. This could be as a healthy part of normal business or for reasons less wholesome but, regardless of the root cause, this organic redistribution of control carries risk and needs to be identified. The delegating person may be avoiding the responsibilities for which they are being employed. The person delegated to may find themselves with responsibilities, sometimes far in excess of their defined role, without adequate support, experience, vetting or training.

3.8 When someone succeeds under these circumstances it can be hard to identify as business will often continue as normal and unscrupulous people will be keen to take credit for the successes of others. If corners are being cut to achieve this then that may cause problems in the future, possibly after the protagonist has left the organisation. There is also the danger that a lack of recognition, combined with the pressure of added responsibility, can lead to resentment. Ultimately that talented individual may leave the organisation or gain a sense of entitlement, which with the right opportunity can lead to detrimental activity.
CONCLUSION

4.1 Through history we have seen that intelligence has been a well valued commodity. Time and again we see evidence of how it has been used to win wars, grow power and influence, build wealth and gain a competitive advantage over our rivals. People once had to go to great lengths for its acquisition and have even killed or died for it. Even so, for some a commodity in abundance loses its value and data has never been as freely available as in the Information Age. But data is not intelligence. Intelligence is the product of processed information and if history remembers those who fail to exploit it, it is only to serve as a bad example.
Global research shows that fraud (and error) costs organisations an average of 5.7% of expenditure but also that this figure varies considerably according to how well protected they are. Key to that protection is having an understanding of the networks within an organisation and the capacity to detect inappropriate or undisclosed networks.

BDO use communications data to identify key nodes within an organisation. This can include telephone data, email traffic or instant messaging depending on your requirements. Raw telecommunications data can be challenging to work with but our specialists apply intelligence techniques adapted from the security sector, to undertake a non-intrusive analysis.

Without examining any of the content of the communications, we can use your data to produce a visualisation of the communications network using specialist intelligence software and visual analysis techniques. Creating a visual communications roadmap from the data will give you the opportunity to see the real flow of information through your business, offering a better understanding of what networks are really operating.

Social Network Analysis (SNA) techniques can be used to identify the critical nodes that may be in a position to control the flow of information. SNA is currently used in the security sector to identify leadership elements, facilitators and other key players. This is done by looking at each node’s position in the network in relation to each other node and assigning it a number property, scores, or centrality measures, based on its relative position. These property scores can give insight into that node’s role or influence in the network.

BDO’s specially trained intelligence analysts can apply SNA to develop a communications roadmap and to highlight key players in your communications network. Not only is this useful business intelligence but it can uncover previously unknown vulnerabilities. Comparing communications patterns with a timeline of key events (for example the issue of invitations to tender or the award of contracts) can be highly successful in revealing potential fraud and corruption.

By combining specialist skills and practical experience... BDO bring together a unique combination of specialist skills and practical experience to ensure that your organisation is properly protected against fraud. We let the data speak for itself, offering a cost-effective Communications Mapping service which helps you to understand the networks within your organisation. We provide a confidential report which ensures you know what is really happening.

We answer your questions.

To find out more, please contact Jim Gee t: +44 (0)20 7893 2830 or e: jim.gee@bdo.co.uk
About the Authors

Jim Gee is Director of Counter Fraud Services at BDO LLP, the leading accountancy and business services firm and Visiting Professor and Chair of the Centre for Counter Fraud Studies at University of Portsmouth. During more than 25 years as a counter fraud specialist, he led the team which cleaned up one of the most corrupt local authorities in the UK – London Borough of Lambeth – in the late 1990s; he advised the House of Commons Social Security Select Committee on fraud and Rt. Hon. Frank Field MP during his time as Minister of State for Welfare Reform; between 1998 and 2006 he was Director of Counter Fraud Services for the Department of Health and CEO of the NHS Counter Fraud Service, achieving reductions in losses of up to 60% and financial benefits equivalent to a 12.1 return on the costs of the work. Between 2004 and 2006 he was the founding Director-General of the European Healthcare Fraud and Corruption Network; and he has since worked as a senior advisor to the UK Attorney-General on the UK Government’s Fraud Review. He has also worked with a range of healthcare organisations, companies and charities as well as delivering counter fraud and regulatory services to companies both in this country and internationally. His work has taken him to more than 35 countries to counter fraud and he has recently been advising the Chinese Government about how to measure, pre-empt and reduce the financial cost of fraud. 2013 has seen him author a book – ‘Countering Fraud for Competitive Advantage’ – with Professor Mark Button which has been published by Wiley.

Professor Mark Button is Director of the Centre for Counter Fraud Studies. He has written extensively on counter fraud and private policing issues, publishing many articles, chapters and completing four books with one forthcoming: Private Security (published by Perpetuity Press and co-authored with the Rt. Hon. Bruce George MP), Private Policing (published by Willan), Security Officers and Policing (Published by Ashgate), Doing Security (Published by Palgrave), and Understanding Fraud: Issues in White Collar Crime (to be published by Palgrave in early 2010 and co-authored). With Jim Gee he has recently written a book (published globally by Wiley) called ‘Countering Fraud for Competitive Advantage’. This highlights the financial benefits to be obtained from countering fraud effectively. He is also a Director of the Security Institute, and Chairs its Academic Board, and a member of the editorial advisory board of ‘Security Journal’. Mark founded the BSc (Hons) in Risk and Security Management, the BSc (Hons) in Counter Fraud and Criminal Justice Studies and the MSc in Counter Fraud and Counter Corruption Studies at Portsmouth University and is Head of Secretariat of the Counter Fraud Professional Accreditation Board (CFPAB). Before joining the University of Portsmouth he worked as a Research Assistant to the Rt. Hon. Bruce George MP specialising in policing, security and home affairs issues. He completed his undergraduate studies at the University of Exeter, his Masters at the University of Warwick and his Doctorate at the London School of Economics. Mark has also worked on a research project funded by the National Fraud Authority and ACPO looking at victims of fraud.
SteveKelly is Assistant Manager, Advanced Data Analytics at BDO (LLP) the world’s fifth largest accountancy organisation. He is an experienced intelligence analyst and, working with the counter fraud team, is responsible for using complex data sets to identify the organisational vulnerabilities that may allow fraud to take place.

Steve’s intelligence background originates from HM Forces where he trained as a soldier and an Operator Military Intelligence. During his early years of service he performed a counter intelligence role on the UK mainland, assessing threats to military assets, seeking to improve the means to protect them and conducting investigations where security breaches had been identified. He completed an eight month tour of Kosovo in an operational intelligence role, successfully targeting high profile and hard to reach persons who were suspected of involvement in terrorism and a variety of other associated criminal interests. He was later deployed to Iraq as a counter intelligence specialist, protecting UK assets through the first democratic elections held in the country for 50 years. Upon returning from Iraq he was posted to Intelligence Database Management Company in Northern Ireland where he specialised in the interrogation of complex data sets and developing new analytical techniques.

Since leaving the army Steve has largely stayed in the security sector, providing intelligence support to UK police forces in tackling serious and organised crime groups and guiding strategic direction. Most recently Steve has been delivering training for IBM on the i2 intelligence analysis product suite to meet the needs of a broad range of sectors. He now seeks to bring his skills and techniques into the counter fraud arena.
ABOUT THE PUBLISHING ORGANISATIONS

**BDO**

BDO LLP is a leading accountancy and business advisory firm, employing 3,500 people across 23 locations in the UK. BDO advises clients on tax, audit, and advisory work across a range of sectors, including Financial Services, Retail, Manufacturing, TMT and Not-For Profit. BDO has a clear ambition to be the firm known in the market for exceptional client service, delivered by empowered people. BDO LLP is a member of BDO International, the largest global accountancy organisation aimed at the mid-market, with revenues of over $6bn operating in 138 countries worldwide.

Our forensic services team offers counter fraud, forensic accounting, expert witness and litigation support services on a national and international basis including:

- Fraud resilience checks;
- Fraud loss measurement and reduction;
- Asset tracing and confiscations;
- Business intelligence;
- Forensic IT, including data mining, data imaging and recovery; and
- Fraud and financial investigations.

**www.bdo.co.uk**

---

**The Centre for Counter Fraud Studies at University of Portsmouth**

The University of Portsmouth’s Centre for Counter Fraud Studies (CCFS) was founded in June 2009 and is one of the specialist research centres in the University’s Institute of Criminal Justice Studies. It was founded to establish better understanding of fraud and how to combat it through rigorous research. The Institute of Criminal Justice Studies is home to researchers from a wide cross-section of disciplines and provides a clear focus for research, knowledge transfer and educational provision to the counter fraud community.

The Centre for Counter Fraud Studies makes its independent research findings available to support those working in counter fraud by providing the latest and best information on the effectiveness of counter fraud strategies.
CONTACT
For more details please contact:

JIM GEE
t: +44 (0)20 7893 2830
e: jim.gee@bdo.co.uk

STEVE KELLY
t: +44 (0)20 7893 3597
e: steve.kelly@bdo.co.uk

This publication has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact BDO LLP to discuss these matters in the context of your particular circumstances. BDO LLP, its partners, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members’ names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Services Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO Member Firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

© 2013 BDO LLP. All rights reserved.