Old Dogs, New Tricks

UK economic crime figures show both fraudsters and fraud schemes are maturing

Image by: Stoyan Yotov / Shutterstock.com

55%

Over half of UK organisations have experienced economic crime

44%

of respondents who experienced economic crime in the last two years had experienced cybercrime

18%

of fraud is now committed by senior management

pwc

www.pwc.co.uk/gecs

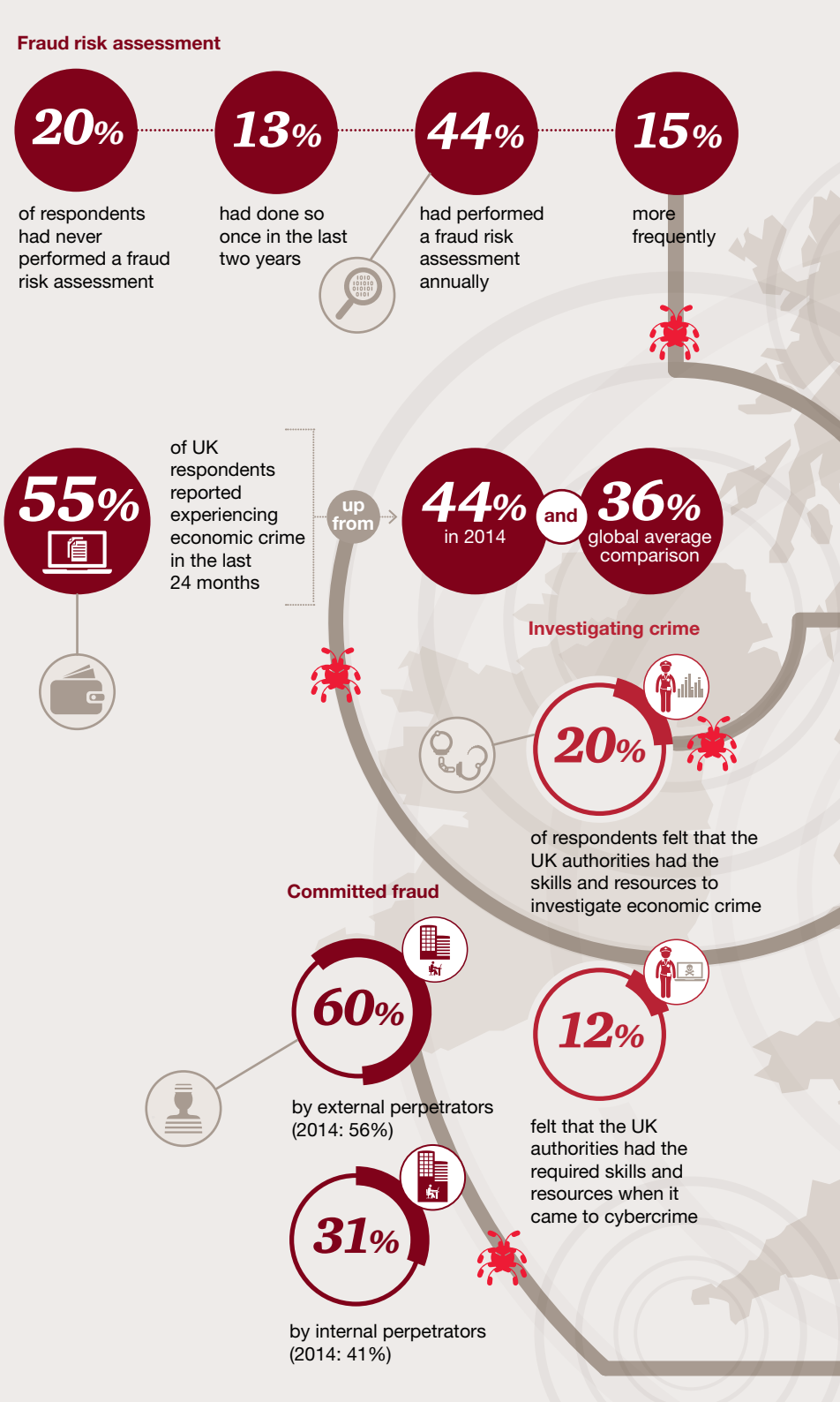
Overview

PwC has been running a global survey of economic crime since 2001, and in that time there has been no significant decrease in the prevalence of fraud. Regulatory regimes have been tightened and billions of pounds have been spent, but economic crime is as tough to tackle as it has ever been.

This year, over half of the respondents to our survey in the UK reported experiencing economic crime, 50% more than the global average of 36%. While the prevalence of traditional frauds such as asset misappropriation, bribery and procurement fraud has fallen since 2014, there has been a huge rise in the number of organisations reporting cybercrime and digital technology is now driving almost every other area of economic crime as well.

While the majority of economic crimes are committed by external parties, a significant percentage of frauds are still being carried out by employees. We're also seeing that the 'typical' fraudster is getting older and more senior, making it more difficult than ever to detect wrongdoing.

The challenge for businesses, then, is to minimise the opportunities to commit economic crime and ensure that there is a robust fraud risk assessment framework in place. This means keeping up-to-date on new threats and new ways to prevent, detect and respond effectively to those threats. It's also vital to ensure that the organisation has a culture based on a strong shared purpose and set of corporate values, which is supported by robust policies, and a rigorous behaviours-based ethics and compliance programme which is integrated into day-to-day operational decision-making.



Ethics and compliance

86%

of respondents have a formal **ethics and compliance** programme in place

Top 5 types of fraud:

- **16%** Accounting fraud (UK 2014: 14%)
- **17%** Human Resources fraud (UK 2014: 13%)
- **18%** Procurement fraud (UK 2014: 22%)
- **44%** Cybercrime (UK 2014: 24%)
- **49%** Asset misappropriation (UK 2014: 65%)

Bribery

5%

have been asked to pay a bribe in the last two years

7%

of respondents felt they had lost an opportunity to a competitor who was willing to pay a bribe

1

People and culture – do you encourage people to do the right thing or to do things right?

The many corporate scandals that have emerged over the last year have proved – if we didn't know it already – that economic crime is also a question of culture, not just a question of compliance. Even the most rigorous compliance programme will fail, if a company's culture allows or accepts wrong-doing as an acceptable way to do business.

- Nearly 1/3 of reported frauds were **committed by staff** with many more involving some degree of collusion.
- We've seen the rise of the **'silver fraudster'** with the percentage of frauds committed by older and more senior employees rising significantly since 2014.
- While the vast majority of organisations have a code of conduct in place, far fewer organisations back this up with regular training and communication.

The UK survey results show that nearly 1/3 of all economic crimes reported in the last two years were committed by staff. Many more may have involved some degree of collusion, often unintended, between outsiders and employees. Frauds that staff typically commit – such as accounting and HR fraud, like falsifying expenses and commission payments – have risen in number in the last two years. While middle management still remain the most likely fraudsters, we have seen a definite shift towards fraud by more senior and more experienced employees: those committed by senior management have more than doubled from 7% to 18%. Similarly, our survey shows the rise of the 'silver fraudster': half of the frauds committed by staff are committed by employees over 40 and the number committed by employees over 50 has tripled in the last two years, from 6% to 18%.

Organisational fraud

31% of frauds in the last 24 months were committed by staff

Level of fraudster in the organisation

Behavioural research tells us that we're less likely to be influenced by rules as we get older, and more likely to act according to our experience and the ways we've always behaved in the past. We are able to rationalise our actions based on previous outcomes – but this may not be the right thing to do. In other words, the older we get, the more willing we are to break the rules and to act according to our own personal moral compass. This is a vital insight when it comes to compliance, because it suggests that more rules are not the answer: in fact you need to strengthen and optimise the working culture through strategic alignment of corporate purpose, values and desired behaviours, and thus reinforce what the organisation – and other key stakeholders – expects.

The vast majority of respondents to our survey (86%) reported that their organisation had a formal business ethics and compliance programme in place. The effectiveness of this programme is often measured through internal audit (80%) and management reporting (67%).

pwc

How do staff really feel?

Organisational values are clearly stated and well understood – **86% agree**

There is a Code of Conduct that covers key risk/policy areas and sets out the organisational values and the behaviours expected of all in the organisation – **89% agree**

Training on the Code of Conduct and supporting policies is provided regularly, supported by regular communications and various advice channels – **63% agree**

Ethical business conduct is a key component of our HR procedures, including objectives, promotion, reward, recognition and disciplinary procedures – **80% agree**

Senior Leaders and Managers convey the importance of ethical business conduct in all they do, setting a positive example and treating it as a priority – **81% agree**

Irrespective of level, role, department or location, rewards are fair and consistent – **64% agree**

Irrespective of level, role, department or location, disciplinary procedures and penalties are consistently applied – **69% agree**

While it is reassuring to see how many organisations understand the value of having a Code of Conduct, it's vital to back it up by targeted, risk-based and experiential education that engages the learner and regular communication from leaders that is relevant and timely. Generic training runs the risk of becoming a box-ticking exercise and a lack of meaningful 'tone from the top' communication from leaders will result in too little impact on actual behaviour. But our survey shows that too many organisations are not doing this.

The responses also highlight another area where organisations are struggling, which is embedding ethical behaviour in the HR processes and, in particular, the reward and disciplinary processes. This is a critical behavioural reinforcement that is required, to support the establishment of an ethical working culture that encourages, motivates and incentivises the right behaviours with appropriate sanctions and rewards.

Taking a public stand against corruption

While the overall level of bribery and corruption that UK companies are reporting has fallen since 2014, it is still a key issue for many boards, not least because of the risk of corporate liability for failure to prevent bribery under the UK Bribery Act.

98% of the respondents to our survey said that their company's management were clear in their condemnation of bribery, and 94% felt that management would rather a business transaction fail than resort to bribery to secure it.

Interestingly, while 85% (globally 81%) of respondents felt that management required business partners to take a public stand against corruption, only 77% (globally 80%) felt that their own management took such a stand. There seems to be a certain double standard here.

How can we help?

Spotlight® is a part of an assessment process and is a web-based tool that allows you to quantify the ethical and compliance risks in your organisation that could arise from the way employees behave. It can help to identify any gaps between (1) the intended behaviours and desirable actions of your staff ('what you want your people to do') and (2) how this is interpreted by line management and supported by reinforcing policies, procedures and processes in place ('how this is expressed in day to day operations'). Any mis-alignment between these results in a risk that your people are not doing the right thing. The bigger the gap, the greater the risk.

The tool is part of an end to end methodology, based on an online survey, which is then analysed with data from in-depth interviews, focus groups and document review to produce a full, measurable assessment of the behavioural risk in your organisation, as well as an evidence-based evaluation of the impact of your ethics and compliance programme on the behaviours and decisions made by your employees.

pwc

2

Making your compliance budget work harder

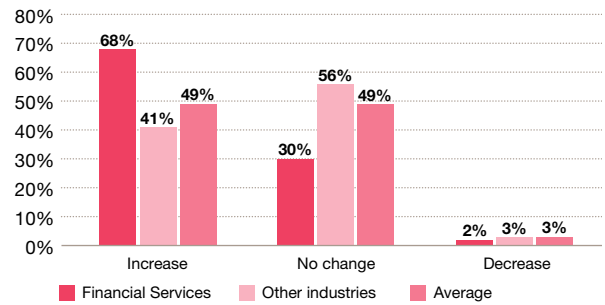
For most organisations, it is a question of when, not if, they will experience economic crime. As the survey results show, the risks companies are facing are not just increasing but becoming more complex, and as the authorities struggle to keep pace, the regulatory burden is growing too. And the threat is diversifying; nearly 1/3 of economic crimes are committed by employees but businesses are also being targeted by agents, customers, vendors, hackers, organised criminal gangs and unknown third parties. An increasing number of incidents involve technology, with a big rise in cybercrime in the last two years.

- 55% ***of our survey respondents said they'd suffered economic crime*** in the last two years.
- ***2/3 of frauds are committed from outside the organisation*** including customers, vendors, agents and other third parties.
- Nearly half of UK organisations have increased their ***compliance spend*** in the last two years.
- 1/5 of respondents had not carried out a ***fraud risk assessment*** in the last two years.

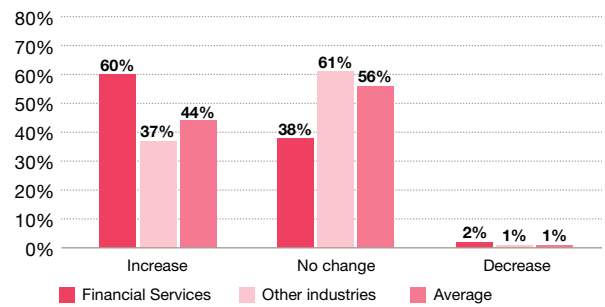
Against this backdrop, nearly half of UK organisations have seen an increase in their compliance spend in the last 24 months and nearly as many – 44% – are expecting an increase in the next two years.

Unsurprisingly, a larger proportion of the organisations spending more on compliance are in the financial services sector, where the level of regulation and oversight requires substantial investment. For other industries, compliance budgets are coming under increasing pressure and compliance functions are being asked to do more with fewer resources.

Compliance spend over the last 24 months



Planned compliance spend over the next 24 months



The most successful organisations understand that there's a commercial and strategic argument for embedding compliance throughout their organisation, and that compliance should be seen as an enabler to good business. At the same time, traditional models of compliance are having to evolve with the new threats and an ever-changing environment. Investment in compliance has to be spent wisely, and on the right things. This includes new skills and capabilities, and technological tools that can handle vast amounts of data, and identify trends proactively.

How can we help?

Procurement fraud remains the third most commonly experienced fraud in the UK, and some sectors (such as transportation & logistics and aerospace & defence) have experienced big rises in bribery and corruption, often involving third parties.

Radar is a real-time risk intelligence monitoring tool which efficiently scans electronic data across foreign languages to detect negative information connected with a company, individual or organisation so that you have a better idea of who you are doing business with, and which third party relationships represent the biggest risk.

pwc

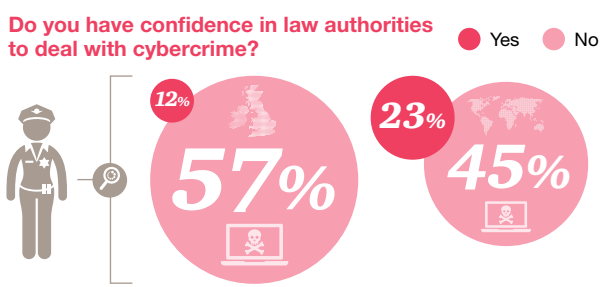
Fraud risk management remains successful in the UK, detecting 14% of frauds compared to the global average of 8% however, as many as 1/5 of respondents said that they had not carried out a fraud risk assessment in the last two years. In this rapidly changing environment where the risks of economic crime are coming from an increasingly diverse number of sources, internal controls and processes cannot remain static. Understanding where the current and potential future threats are can help companies to keep one step ahead of the fraudsters.

What should management think about when considering economic crime?

- When was the last time you conducted a thorough fraud risk assessment?
- What does the 'right size' fraud risk assessment look like and consider?
- To what extent have current fraud trends, either sector specific or otherwise, been identified and considered?
- Is the organisation's assessment of fraud exposure documented and comprehensive?
- How has fraud risk been measured, and against what criteria have you determined inherent and/or residual risks to be acceptable with regards risk appetite?

What happens when a fraud is committed?

With the rate of economic crime in the UK rising, our survey shows a low level of corporate confidence in law enforcement agencies' ability to deal with economic crime, and one that's lower than the global average. Confidence is particularly low when it comes to dealing with cybercrime.



Using data more effectively

Our survey shows that 30% of reported frauds were detected by suspicious transaction monitoring or data analytics. Rather surprisingly, this is down from 37% in 2014. Organisations clearly aren't producing any less data than they were two years ago, so the focus needs to be using the data generated more effectively and to identify potential frauds more quickly and efficiently.

Some of the more advanced techniques that can be used include:

Searching: Keyword searching across different types of data, and 'intelligent' search queries based on a deeper understanding of the structure of the data.

Screening: Analysis of data to pinpoint specific transactions, as well as rules-based exception testing, statistical analysis and text mining.

Intelligence: The use of technology to capture and organise the knowledge acquired in investigations, and to track ongoing lines of enquiry.

Graphing: The analysis and visualisation of communications and relationships, providing a new perspective on familiar data.

It's also important to remember that technology alone will not detect economic crime: the results will depend on the quality of the underlying information and require human intervention to review the results and investigate further.

Given the low levels of confidence in law enforcement, it's not surprising that the vast majority of respondents (83%) would begin by performing an internal investigation if they discovered a potential fraud. A significant number of respondents also turn to third parties such as external auditors (32%), legal advisors (22%), or specialist forensic investigators (14%).

How can we help?

identify is an interactive health-check application designed to uncover fraud across expenses, payroll, and procurement. It combines intuitive dashboards and advanced data analytic techniques such as employee profiling and text mining, allowing you to review and investigate suspicious payments, anomalous activity, and non-compliant behaviour.

pwc

3

Cybercrime

Cybercrime is one of the headlines of this year's global survey, which is no surprise, given it has been in the news for months now. It's also the type of economic crime that shows the most significant increase in prevalence since 2014.

As businesses become ever more reliant on technology, and hold more and more information about their business, customers and clients, there are huge opportunities for cyber criminals to exploit weaknesses and gaps in controls.

This is an area where the UK is ahead of the trend in all the wrong ways: 44% of UK respondents who had suffered economic crime in the last two years had also been the victim of some sort of cyber incident. That's up from 24% in 2014, and is much higher than the global average of 32%. This finding is consistent with other research which shows a large increase in the number of detected incidents in the UK over the last few years. Over half of the UK survey respondents think it's likely that they will suffer from cybercrime in the next two years as well, with 71% of respondents saying the risk has increased over the last two years.

Where does the threat come from?

Nearly 2/3 of respondents to our survey (65%) believe the threat of cybercrime comes primarily from outside the organisation. However, PwC's recent Global State of Information Security report shows that there has been a 58% increase in the number of employee-related security breaches.

When considering the threat of cybercrime, organisations must take into account the human element. Many cybercrimes are, at heart, just old fashioned confidence tricks. Which means even the strongest IT controls cannot always protect you.

44%

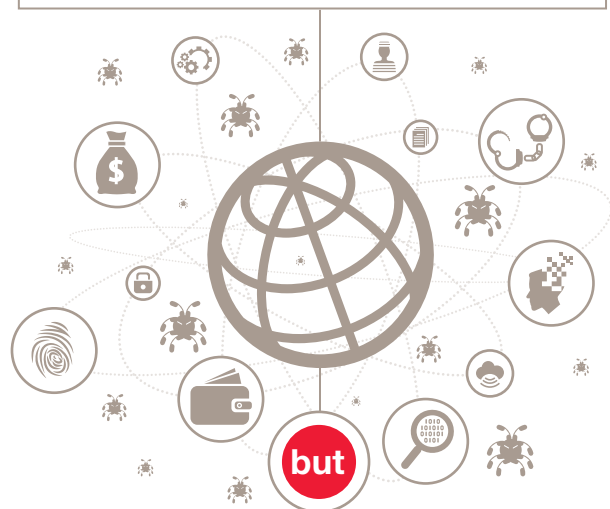
of UK respondents who reported experiencing economic crime in the last 24 months reported experiencing cybercrime, up from 24% in 2014.

71%

felt the risk of cybercrime had increased over the last two years.

51%

of respondents felt that they would be likely to experience cybercrime in the next two years.



12%

of respondents in the UK felt that law enforcement had the required skills and resources to investigate cybercrime

30%

of organisations don't have a cyber response plan in place.

pwc

One reason for the steep increase this year is the increasing take-up of cloud-based storage, and the growing prevalence of the 'internet of things', with everything from fridges to office coffee machines connected to a network and therefore vulnerable to hackers. And those hackers are more ambitious than ever before, targeting not just credit card or financial information but the sort of 'crown jewels' that can bring down an entire business if they're stolen, whether that's intellectual property, commercially sensitive information, or operational data that can be encrypted by malware and held to 'ransom' until the victim pays to get it back.

The most significant conclusion to be drawn from all this is that cybercrime is no longer just an IT problem. It's a major business risk, and has to be managed accordingly. That means having the right people, the right processes, and the right governance, fortified with the right technology. It means making cyber issues an integral part of routine risk assessments, with active oversight from the Board. But at the moment only 25% of the organisations that we surveyed said that their Board actively requested this information or felt the need to request it.

The importance of a response plan

43% of the survey respondents said that they have a fully operational cyber attack response plan, which is higher than the global average of 37%. This may be because only 12% of respondents in the UK feel that the law enforcement agencies have the ability and resources to investigate cybercrime, compared to 23% globally.

Despite the number of high-profile cyber breaches in recent months, as many as 30% of respondents said their organisation has no response plan, although 2/3 of these respondents are currently assessing the feasibility of implementing such a plan. Given that it's more a matter of when you're attacked than if, all organisations should have a response plan that is relative to the size of the organisation and scaled according to its needs and budget. This is particularly important if you hold any kind of confidential data, which should be protected as a priority.

Those organisations that do have response plans must ensure they test them regularly and update them as needed. Robust testing may help to identify weaknesses, or gaps which may not have been considered, such as the allocation of roles and responsibilities.

Cyber is another area where data analytics can be helpful to identify key risk areas and monitor incoming traffic, so long as sufficient time and money is invested in analysing the data produced. Full visibility will help you to manage risks across the whole business.

The impact of cybercrime

Nearly half of those who had suffered cybercrime in the last two years told us that they had experienced no financial lost as a result of the cybercrime attack. In our experience though, the true financial loss in these situations can take years to quantify and it's often the collateral impact that does the real damage.

The biggest concern about a cybercrime attack for our survey respondents is the potential service disruption (31% said it would have a high or medium impact) on the business. Surprisingly, nearly half of respondents said that a cybercrime would have no impact on their reputation and 58% were not concerned about the potential for the theft of IP. In our view, it's impossible for a cybercrime not to have an impact on an organisation's reputation or it's IP.

How can we help?

PwC provides a full spectrum of services to help clients prepare for, detect, investigate, and remediate cyber incidents associated with the modern threat landscape.

We can help you build a cyber crisis capability, including:

- a crisis framework - outlining analysis and decision making guidelines to underpin an organisational response;
- threat profiling – identifying the real-world threats you face in order to enable you to tailor your preparation efforts appropriately;
- playbooks – step by step technical and management guidelines for specific incident types; and,
- forensic readiness – ensuring you have the right data available and accessible to be able to thoroughly investigate an incident.

We also have a threat intelligence reporting service that provides updates on a wide variety of threat activity, from summaries of techniques and malware families to geopolitical influences on threats. Our research covers not just espionage but also cybercrime and hackers-for-hire. We are also able to help detect financially motivated attacks through our detection and monitoring services.

Our cyber security services go far beyond the crisis and incident space to help you build and assure your defences, as well as navigate the legal and regulatory data privacy landscape.

pwc

Mark Anderson
Partner, Global Corporate Intelligence Leader
T: 0207 804 2564 M: 07770 921256
mark.r.anderson@uk.pwc.com

Tracey Groves
Partner, Compliance & Business Ethics
T: 0207 804 7131 M: 07803 853425
tracey.groves@uk.pwc.com

Kris McConkey
Partner, Cyber Threat Detection & Response
T: 0207 804 2471 M: 07725 707 360
kris.mcconkey@uk.pwc.com

Andrew Gordon
Partner, Global & UK Forensics Leader
T: 020 7804 4187 M: 07803 234252
andrew.gordon@uk.pwc.com

Ian Elliott
Partner, Head of Investigations
T: 020 7213 1640 M: 07711 912415
ian.elliott@uk.pwc.com

Survey Editorial Team:

Keith McCarthy, Director
T: 020 7804 3914 M: 07775 672456
keith.v.mccarthy@uk.pwc.com

Kathryn Westmore, Senior Manager
T: 020 7213 2941 M:07715 211090
kathryn.m.westmore@uk.pwc.com

Bonnie Whang, Senior Associate
T: 020 7212 2002 M: 07525 282316
bonnie.whang@uk.pwc.com

Survey Marketing Team:

Gill Hemming, UK Marketing Manager
T: 011 3289 4255 M: 07715 033797
gillian.hemming@uk.pwc.com

"Whilst the SFO is not in the business of giving advice, the best ethics and anti-corruption programmes are surely those which are simply stated, inculcated by training, energetically enforced and lived by all in authority. A thick policy book, carefully lawyered but ignored in practice is as bad as no policy at all."

David Green, Director, Serious Fraud Office

www.pwc.co.uk/gecs

The Design Group 30308 (02/16)