Out of the shadows

Spotlight on public sector fraud

SEPTEMBER 2017

CIPFA The Chartered Institute of Public Finance & Accountancy

PF Perspectives

This is the sixth in a series of *PF Perspectives*, produced by CIPFA and *Public Finance*. They are designed to stimulate discussion on key public finance and policy issues. These essays, by leading public sector practitioners and experts, examine the far-reaching implications of fraud for public sector organisations and discuss strategies to detect and counter it

CONTENTS

FOREWORD

ROB WHITEMAN
Chief executive of CIPFA

Redactive Publishing Ltd
Level 5
78 Chamber Street
London E1 8BL
020 7880 6200
www.publicfinance.co.uk

redactive

Editor
Judy Hirst

Design
Gene Cornelius

Chief sub-editor
Christy Lawrance

Illustrations
Dan Funderburgh,
Paddy Mills

Printing
Stephens and George
Merthyr Tydfil, Wales

CIPFA The Chartered Institute of Public Finance & Accountancy

Tel 020 7543 5600
Fax 020 7543 5700
www.cipfa.org
CIPFA, 77 Mansell Street,
London, E1 8AN

ISSN 2058-1777

Fraud is a massive and growing problem. Yet it is rarely gets the public attention it deserves.

Whether we are talking about unscrupulous scammers preying on vulnerable older people, or criminal insiders defrauding companies of billions, the human and financial costs are huge.

For the public sector, fraud is a particular affront. Public services, paid for from taxpayers' money – and severely stretched by years of austerity – can ill afford to be ripped off by fraudsters. They need better protection if they are to survive.

The recent ransomware attack on the NHS was a wake-up call. It demonstrated the ever-changing nature of the threat of global cybercrime. We need to get a lot smarter than the fraudsters if our services – and the users who depend on them – are not to be put at risk.

There have already been encouraging moves in this direction. CIPFA's counter-fraud centre, in conjunction with government, has been promoting local hubs that collaborate on combating fraud through the use of analytics.

New legislation on data protection, and Cabinet Office initiatives on counter-fraud professionalisation, are coming on stream. The annual counter-fraud awards demonstrate there is much to celebrate in this regard.

There is also a growing awareness that fraud must be treated as a top table, strategic issue, rather than being left to the back office. And that, when it comes to taking on the fraudsters, prevention and awareness training are key.

But, as this important essay collection indicates, there is still a long way to go.

The causes and remedies for fraud are complex and systemic. Many of the challenges involved with public sector transformation apply equally when it comes to tackling fraud.

As the OECD's deputy head of public sector integrity argues persuasively (page 26), tackling fraud and corruption is closely connected to the wider problem of restoring public trust.

This is particularly relevant to the issue of whistleblowing, and the need to encourage transparency about public sector wrongdoing.

It is also relevant to areas such as tax abuse and procurement fraud, which not only hit the public purse harder each year, but are particularly tough nuts to crack.

Nevertheless, a start has been made. By bringing fraud out into the open – and calling out the perpetrators - public sector professionals perform a vital service for society at large.

Fraud is, at last, the issue that dares speak its name. The test now is, how effectively can we deal with it?

CONTRIBUTORS

ROB WHITEMAN

Rob Whiteman is chief executive of CIPFA. He previously led the UK Border Agency and the IDeA, and was chief executive at Barking & Dagenham Council

CHRIS SKIDMORE MP

Chris Skidmore is Minister for the Constitution. His Cabinet Office remit includes fraud, debt and grants

MARGARET HODGE MP

Margaret Hodge MP is chair of the All-Party Group on Responsible Tax and was chair of the Public Accounts Committee from 2010 to 2015

SIMON DUKES

Simon Dukes is chief executive of fraud prevention service Cifas. He was previously a senior manager in central government

RACHAEL TIFFEN

Rachael Tiffen is head of the CIPFA Counter Fraud Centre. She previously managed the Ministry of Defence's Counter Fraud Service

MARK CHEESEMAN

Mark Cheeseman is deputy director, public sector fraud, at the Cabinet Office. He was previously head of fraud and error policy

IAN O'DONNELL

Ian O'Donnell is executive director of corporate resources at Ealing Council. He is lead for the London Counter Fraud Hub

ANTHONY HARBINSON

Anthony Harbinson is chair of the Fighting Financial Crime Task Force of the Consultative Committee of Accountancy Bodies

JULIO BACIO TERRACINO

Julio Bacio Terracino is deputy head of public sector integrity at the Organisation for Economic Cooperation and Development

ANDREW ROSE

Andrew Rose is senior policy officer responsible for public sector engagement at the Information Commissioner's Office

GARY WALKER

Gary Walker is an adviser on governance, a Public Concern at Work trustee and a former NHS chief executive and whistleblower

KATY WOROBEC

Katy Worobec is head of fraud and financial crime prevention, cyber and data sharing at UK Finance and a co-founder of the Fraud Women's Network

FACING UP TO FRAUD

On the offensive

ESSAY

BY CHRIS SKIDMORE MP

A robust counter-fraud strategy is being developed by government, to tackle the new threats faced by public services

Chris Skidmore *is minister for the constitution. His Cabinet Office remit includes fraud, debt and grants*

THE GOVERNMENT'S ROLE is to protect public services and countering fraud is an important part of this protection. The annual Crime Survey of England and Wales said earlier this year that fraud had become the most prevalent crime in the UK. There has never been a more appropriate time to focus on the fight against public sector fraud.

As the pace of technology and consequently cybercrime have increased, fraud is becoming a progressively common risk in our everyday lives. It comes in the form of brazen telephone calls attempting to get your bank details, to false pretences, to the ubiquitous scam email. All individuals and organisations are at risk of financial loss through fraud, and the UK public sector is no exception.

The public sector has a great challenge in countering fraud. The work of government is hugely varied and complex. Our work involves interactions with millions of customers and providers every day, through a diverse range of services and systems. Good government is about ensuring well-run and affordable public services for all, so it is critical that risk to fraud is countered by a robust, proactive counter-fraud approach.

Effectively countering fraud against public services remains a priority for the government. The UK is rightly proud of its record in fighting fraud and corruption both in the public sector and more widely – we have already made significant strides in this area, and our fraud figures on tax and welfare are scrutinised and published annually. To realise this priority, the government is undertaking significant activity to reduce fraud in the public sector; for example, we continue to run the National Fraud Initiative, which focuses on the prevention and detection of fraud through matching and analysis of electronic data.

Curiosity kills the crimes

I am urging public servants to "be more curious" in their approach to fraud and take an active part in helping to tackle it. Everyone has a role to play in countering fraud, whether they are board members, senior managers, frontline staff or those delivering public services. Everyone has a responsibility to see the risks in their area of the business, to avoid complacency and remain vigilant. Finding fraud benefits not only the organisation where it is taking place but also government and society more generally. It means a more fair and just society as well as money returned to the public purse.

We are seeking out fraud in all its forms. The UK government has already begun and is committed to a number of key initiatives in the fight against public sector fraud. I am proud of the work of the Counter Fraud Centre of Expertise at the Cabinet Office, which brings together the cross-government counter-fraud response by working collaboratively with departments on common issues.

The team has already carried out excellent work in its drive to improve capability across central government. Perhaps most exciting is the development of a government Counter Fraud Profession, which is due to be launched within a year; this will focus on improving capability across government through the creation and adoption of Counter Fraud Standards and specific products and guidance to enable public sector resources to make a real difference.

A further critical area of the government's counter-fraud response is increasing the use of data sharing and analytics to find more fraud and to proactively prevent it. The Digital Economy Act has been developed to aid this priority and acts as a simple gateway for public authorities to establish data-sharing pilots to counter fraud and enhance collaborative working in this area.

The government's commitment to the fight against public sector fraud has never been stronger with the old belief that fraud is a taboo subject now completely revoked and powerful initiatives – such as the government Counter Fraud Profession and the adoption of standards – promoted and championed across government. Indeed, there are such varied and committed counter fraud initiatives and projects across the public sector that we are proud to celebrate the successes and best examples of these in the annual Government Counter Fraud Awards.

Finding fraud: an achievement

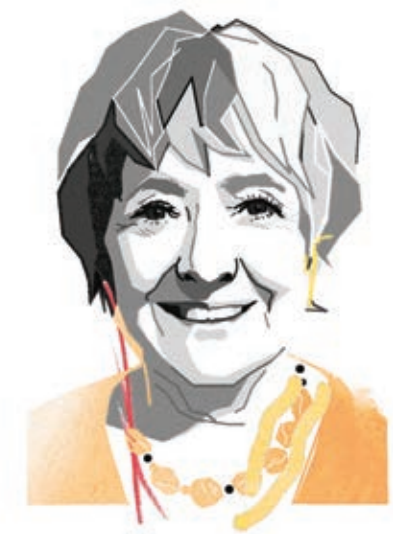
We encourage professionals across the public sector, both specialist and generalist, to play their part in this fight by taking fraud seriously, being curious in their approach towards finding fraud and understanding that finding fraud is positive, so that work can begin to combat the issue.

Fraud is a hidden and complex crime but, by having access to and utilising the right skills and products, as well as modelling the change in narrative on fraud, public servants can aid the government's robust counter-fraud response, thereby protecting public services and ultimately saving taxpayers' money.

'I urge public servants to "be more curious" in their approach to fraud and play a proactive part in helping to tackle it'

Protecting the taxpayers' pound

ESSAY



BY MARGARET HODGE

Tax fraud deprives public services of much-needed revenue. It needs to be tackled more effectively

Margaret Hodge *MP is chair of the All-Party Group on Responsible Tax and was chair of the Public Accounts Committee from 2010 to 2015*

TACKLING TAX EVASION – and avoidance – may not be enough to save our public services, but it is certainly very important. The reason is not difficult to fathom. Public services are funded by taxes paid by individuals and corporations. If individuals and corporations do not pay their fair share, governments will not have enough funds for schools, hospitals and the police. They will then have to choose between borrowing more, spending less, increasing taxes or a combination of the three.

During the time I chaired the Public Accounts Committee (2010-15), the coalition government consistently chose to cut spending to reduce the deficit. The result was catastrophic for our public services. The recent Performance Tracker 2017 study, published by the Institute for Government and CIPFA, shows these cuts meant that since 2010 fewer people accessed state-funded social care although more needed it, and that since 2013 more people have waited longer for cancer treatments. Austerity affects those who are least able to manage on their own the most – families with children, the sick, the elderly, the most vulnerable.

My experience as chair of the Public Accounts Committee taught me that we can avoid some cuts by securing better value from the taxpayers' pound. Our inquiries identified too much unconscionable waste and too little learning from past mistakes, whether it was in public procurement, major IT projects or the running of local services. I have argued that we need to do better and ensure greater efficiency in the use of public money. We need to introduce fundamental reforms in transparency, accountability and civil service competencies and career paths.

HMRC's performance in collecting the tax due goes to the heart of the efficiency and effectiveness of government. If HMRC were more effective in getting the monies due into the public coffers, we would not need such great cuts to our public services to reduce the deficit.

During the five years that I chaired the Public Accounts Committee, we held 20 separate hearings on tax and made more than 100 recommendations to the government that we believed would improve the state's performance.

Much of the focus of our work was on aggressive tax avoidance rather than tax evasion. We discussed at length whether tax avoidance was legal or illegal, moral or immoral. Tax evasion left us with no doubts: it was illegal. There was no grey area, nor a debate about morality to be had.

And evasion is as important as avoidance. Indeed, according to the latest HMRC estimates (2014-15), tax evasion accounts for a substantially larger share of the tax gap than tax avoidance (£5.2bn against £2.2bn). If we trust these figures, the inevitable conclusion is that tackling tax evasion is as important for our public services as tackling tax avoidance.

Mind the gap

However, I share the scepticism of others that the official HMRC figures fail to tell the whole story. Tax campaigners calculate a much bigger tax gap. Professor Richard Murphy from City University, for instance, believes that in 2014 the tax gap was £120bn (including

£70bn in evaded tax and £25bn in avoided tax). This would imply that tackling tax evasion and tax avoidance can be a realistic alternative to austerity.

For my part, I am not confident that we can calculate tax gaps accurately. But the real point is that, whether the estimates are accurate or not, it is obvious that we need to do more to collect the taxes due – especially as this means that we will be forced to do less slashing of public services to cut the deficit.

Everybody agrees that tax evaders should face harsh penalties. If individuals and corporations believe that they can evade taxes with impunity, it will be impossible for any government to convince them to pay their fair share. Personally, I think this has been one of our main problems in the UK.

The Falciani list of HSBC's Swiss branch clients, made public in 2015, showed HMRC's struggle in investigating tax evasion, as well as the competent authorities' hesitation in prosecuting tax evaders – and banks' collusion with them. From around 1,000 HSBC clients domiciled in the UK and under suspicion of tax evasion, only one was prosecuted for this crime.

The Public Accounts Committee was told prosecuting tax evaders was difficult and expensive. I was never convinced by this argument. I believe that threats of a serious accusation in court and the possibility of spending time in prison act as a strong deterrent to those thinking about evading tax.

In 2015, the government announced that it wanted to increase the number of criminal prosecutions to 100 a year. I hope the new mechanisms introduced this year with the Criminal Finances Act 2017 (including the new unexplained wealth orders and the new offence of failing to prevent the facilitation of tax evasion) will lead to more prosecutions of tax evaders, but it is too early to tell.

Public registers

The most significant recent development has been the movement towards transparency and the creation of public registers. If public registers of beneficial owners of companies and trusts were adopted by all jurisdictions, scrutiny over private dealings would be transformed and tax evasion would become much more difficult for individuals, companies and their advisers. Law enforcement bodies and civil society could more easily identify potential crimes and criminals. Such scrutiny would not only prove a genuine deterrent to potential criminals but also increase public trust in government agencies.

For the OECD's head of tax, Pascal Saint-Amans, revealing the secret identities behind corporations and trusts is the "new frontier" in the fight against tax evasion. I agree with him and I strongly support the creation of public registers. That is why our All-Party Group on Responsible Tax is campaigning to persuade the UK government to introduce public registers in the tax havens that are UK overseas territories.

The Panama Papers showed that British overseas territories and crown dependencies have a prominent role in international money-laundering, corruption and tax evasion. But, despite protesting that it favours public registers, the UK government continues to refuse ▶

'If HMRC were more effective, we would not need such great cuts to our public services to reduce the deficit'

to support the All-Party Group on Responsible Tax's campaign on the overseas territories, demonstrating a somewhat hypocritical approach to tax avoidance and evasion.

Public registers are proving controversial elsewhere. On 21 October last year, the French supreme court declared the public register of foreign trusts with assets in France, or with French resident settlors or beneficiaries, was contrary to the Constitution of France. The French government had decided to publish the register publicly in July 2016.

Within a month, this was legally challenged and suspended by the Conseil d'Etat. In October, it was declared unconstitutional by the supreme court on the grounds it disproportionately interfered with the right to private life. "A reference in a publicly accessible register of the names of the settlor, beneficiary and administrator of a trust provides information on how a person intends to dispose of his or her estate," the French judges wrote. And the trust register went back to being private.

Transparent regime

The outcome of the French case did not seem to dissuade others who believe public registers will facilitate the fight against tax evasion, money laundering and other economic crimes.

The move towards public registers gained momentum after the Panama Papers hit the media in April 2016 showing the world how banks, lawyers and politicians collude in hiding wealth and evading tax.

The European Union produced the Fourth Money Laundering Directive (effective since 26 June 2017) requiring member states to create central registers of beneficial owners, and is now working on a Fifth Money Laundering Directive, which may require member states to make those registers public in the future.

Another questionable development is the UK government's decision to introduce a new register for trusts that is not accessible to the public. I honestly cannot see a reasonable explanation for this difference in treatment between companies and trusts.

At the same time, the Department for Business, Energy & Industrial Strategy is consulting on the creation of a public register of beneficial owners of overseas legal entities that own UK property or participate in UK government procurement.

A 2016 report published by Transparency International UK and Thomson Reuters – London Property: a Top Destination for Money Launderers – shows that "land and property in London are popular choices for those looking to launder the proceeds of corruption into the UK".

Progress here is slow and our parliamentary group is determined to maintain the pressure on the government to implement this register in an open way that will truly reveal who owns property in the UK.

Our hope is that we will develop a transparent tax regime in the UK, where the possibility of public scrutiny rebuilds trust between individuals, corporations and our tax administration, and where tax justice and adequately funded public services contribute to a more stable and cohesive society. ●

'If individuals and corporations believe they can evade taxes with impunity, it will be impossible for any government to convince them to pay their fair share'

Into the light

ESSAY

BY SIMON DUKES

Some of the biggest public sector fraud hazards come from within organisations. It's time to openly confront the issue

Simon Dukes *is chief executive of fraud prevention service Cifas*

FRAUD IN THE PUBLIC SECTOR isn't just about false benefit claims or dishonest grant applications. One of the biggest sources of fraud, according to our public sector partners, is to be found within their own organisations – individuals stealing data or money, or taking advantage of their position to corrupt others.

This is shocking but in some ways unsurprising. Criminal activity follows the money and, in the digital economy, data is the new oil. Because they hold a wealth of information on individual citizens, government bodies are under attack from both inside and out.

At Cifas, we are leaders in fraud prevention, which means a whole range of cases are reported to us. We know about staff at public sector bodies who have been reported for diverting money intended for disadvantaged citizens to their own family and friends' bank accounts. And we even have examples where fraudsters within state organisations have used their positions and power to bribe the vulnerable. It is disturbing to hear of staff who force others to commit crimes against their will with the threat of withdrawing their benefits or grants if they don't go through with it.

These cases are clearly at the extreme end of the scale. However, we also know that one of the biggest risks is fraudsters attempting to gain access to an organisation to steal citizens' data. Clearly, this personal information needs to be held so public sector bodies can carry out their day-to-day operations, performing tasks such as paying benefits, making pension payments, adjusting tax codes, funding grants and issuing penalty notices. However this data commands a high price on the outside. Identity fraud hit a record level in 2016, with almost 173,000 cases recorded on the Cifas database, representing over half of all fraud cases we collated.

There are some simple measures an organisation can take to stop dishonest staff leaking client data to malicious third parties. Clear anti-fraud policies that support staff whistleblowing help demonstrate a zero tolerance approach to fraudulent or corrupt behaviour. Smart technology can monitor employees' access to data and systems – providing a useful vapour trail. Being open and frank about instances of fraud helps to bring the issue to light and deter other employees from following the same route. So too does swift and effective action taken against the perpetrator once they are found out.

Of course, no organisation can fully protect itself from insider threats merely by introducing a robust screening process at the job application stage – although this is a good idea. Cifas research has previously highlighted that the average length of service before a fraud is identified is six and a half years. These findings correlate with a study from KPMG which found that 41% of internal fraud is committed by those who have been in the organisation for more than six years.

Low risk, high rewards

Why do they do it? Financial gain is a major incentive of course, whether the fraud is carried out by a serial offender or an opportunist. For organised criminals who abuse and hide behind the identities of innocent parties, fraud is seen as a relatively low-risk activity with potentially high rewards. To them, it appears to carry a lower chance of getting ▶

caught than for other crimes, and a shorter sentence.

Interviews with convicted internal fraudsters found some common themes. Too often, an opportunity presents itself and they did not expect to get caught. Our partner organisations across all sectors frequently report cases where employees move department or job and still have access to systems and data they no longer require. Organisations failing to put the right controls and procedures in place to prevent this are helping potential internal fraudsters access data they are not entitled to. Cifas members also state that drug, alcohol or gambling addictions are the motivation for some of the cases they have identified.

Frauds recorded by Cifas and Financial Fraud Action UK are now included in the Office for National Statistics crime figures. Volumes are now at an all-time high, with almost half of all crime being fraud.

We welcome the introduction of the Home Office Joint Fraud Taskforce , whose efforts have given the government, law enforcement agencies and their partners a renewed focus on the issue. But Cifas continues to call for the tackling of fraud to become a strategic priority for UK police, and for fraud offences to carry a tougher sentence. A greater deterrent would surely help to drive down the huge volume of cases that we are now seeing.

We also want to see fraud education in the national curriculum and every child from 11 onwards receive consistent education on how to protect their identities online and protect themselves from fraud. To that end, Cifas is working with the PSHE Association and will be running a pilot in September with selected schools.

‘Identity fraud hit a record level in 2016, representing over half of all fraud cases we collated’

Collaboration and data sharing

One of the ways Cifas helps organisations is by allowing them to share details of confirmed internal fraudsters through our Internal Fraud Database. This database allows organisations to screen new and existing employees to confirm that no known fraudsters are working for them. It also means that dishonest staff cannot move undetected from one organisation to another and commit further crimes.

Many of those who use the Cifas Internal Fraud Database say that signing up acts as an effective deterrent in itself. It is also why the Financial Conduct Authority, the Chartered Institute of Personnel and Development, Fighting Fraud Locally and others have suggested that using the system is good practice.

Working together like this is relatively new. It is worth noting that it took section 68 of the Serious Crime Act 2007 to establish a legal gateway to permit public bodies to share data through a specified anti-fraud organisation such as Cifas. Since then, large strides have been made.

Cifas is the only organisation that shares confirmed fraud data across public and private sectors. Because we are trusted to collate information supplied by over 400 member firms – including banks, insurers, telecoms providers, charities and public sector organisations - we see hundreds of attempted frauds foiled every day. For the fourth year running, our

cross-sector membership prevented more than £1bn in fraud losses.

While the bulk of our members come from the private sector, our public sector membership continues to grow and now includes, among others, the Home Office, the Student Loans Company, the Big Lottery Fund, the Land Registry and the Charity Commission. We are always keen to sign up more to increase our reach and effectiveness and believe much is to be gained from the public, private and third sectors working together on what is essentially a non-competitive issue.

There are other initiatives that we are involved in. From next year, the 33 London boroughs will be able to access Cifas data and share their own fraud data with Cifas members through the CIPFA-managed London Counter Fraud Hub.

This is a great example of how collaboration between the public and private sectors can combat fraud and the organised crime it funds. At the heart of the hub is an analytics solution that helps prevent, detect and recover losses from fraud. It also offers a range of services to ensure teams have the optimal level of resources, know-how and support. We would like to see this level of collaboration repeated across the country.

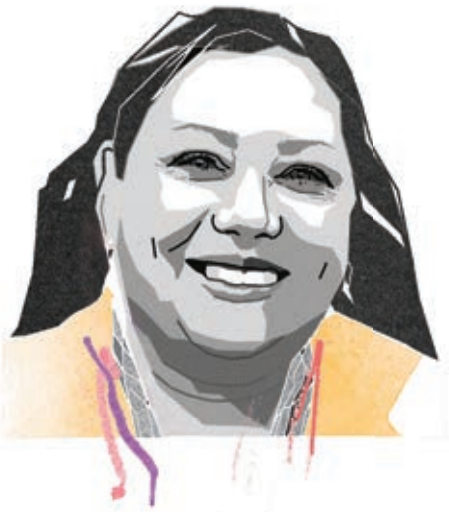
As well as going wider, organisations should go deeper by sharing information beyond raw offender data. Trends, typologies and methodologies can help to identify where the next threat may come from and tighten up processes. Cifas runs a number of free Organised Fraud Intelligence Groups around the UK, where organisations from the public, private and charity sectors can learn from each other in cooperation rather than competition.

The drive to further digitise public services means that the data coveted by criminals will only increase in quantity. As well as protecting ourselves from external fraud threats, we must be prepared to tackle the internal danger that threatens to compromise the effectiveness and reputation of our key public bodies. It is in the public interest to do so.

‘Criminal activity follows the money and, in the digital economy, data is the new oil’

A top table issue

ESSAY



BY RACHAEL TIFFEN

Tackling fraud is the responsibility of everyone, whether in the biggest or the smallest organisations. So why isn't it higher up board room agendas?

Rachael Tiffen *is head of the CIPFA Counter Fraud Centre*

AT THE START OF 2017, I did some horizon scanning. Some of the things that were on my hit list have materialised or are being addressed. Others are still waiting to happen. Meanwhile, new threats emerge all the time.

My topline themes included: shaking up the data protection laws; stopping fraud at source; digital transformation to tackle cyberattacks; coping with the limited resources that strangle counter-fraud initiatives; and – most important of all – making sure counter-fraud strategy was set and owned from the top down.

It's not too hard to work out the key strategic trends. The impact of fraud and corruption on the public sector and on communities has been well documented in recent times. The urgency of raising awareness of common types of fraud, along with identifying and preventing fraud and corruption in the first place, has gained wider currency over this past year.

It is also important to have a holistic view of public sector fraud because the risks that arise in local government can occur in central government too, and vice versa. What is done to tackle them and the input might be different but, by working together more, we can make the first steps so much easier.

CIPFA produces an annual Counter Fraud and Corruption Tracker (CFaCT), which allows us to drill down for details. The data for 2017 shows an increase in counter-fraud activity in the area of fraud investigation – more than £336m was investigated compared to £325m in the previous year.

The findings also show a lack of funding continues to dominate decision making about strategic direction and implementation. However, improvements in shared services, technological advances, national, regional and local initiatives – and alternative funding routes – all have the potential to enable improvements in the fight against fraud.

The emergence of data analytics hubs is welcome. This is an acknowledgement of the recommendations in *Fighting Fraud Locally*, the counter-fraud strategy for local authorities that was published in 2011 by the government and updated by CIPFA in 2016. This addressed fraud prevention and collaboration through the use of data analytics. It also recommended that councils took up the idea of data hubs and many have begun to do this.

CIPFA is playing another role in this area too, having won the contract to deliver the London Counter Fraud Hub, and is now working with many councils on similar initiatives. This demonstrates the appetite at a number of levels to change culture.

Cybercrime

Most public sector organisations are deeply concerned about the growing use of cyberattacks to perpetrate fraud. You have only to look back over the past year to see what a damaging impact such attacks can have on an organisation.

In May 2016, a hacker advertised more than one hundred million LinkedIn logins for sale. The information, including email addresses and passwords, had been obtained from a breach four years earlier. In April 2017, Wonga was the victim of a data breach, with up to 250,000 accounts compromised. Then, on 12 May 2017, the public sector was directly

affected, when the NHS was hit by the WannaCry ransomware attack.

Hospitals and GP surgeries in at least 16 health services in England and Scotland were severely disrupted, with patients turned away, appointments cancelled and staff forced to resort to pen and paper and using their own mobile phones.

This was part of a much wider cyberattack in 150 countries, in which malware was used to encrypt files with sensitive data, followed up by bitcoin ransom demands. Although the actual cost of the ransomware attack may not have been that high, the damage and costs incurred by forensic investigations, loss of productivity, security checks and restoring data were considerable. In answer to a parliamentary question, care minister Jackie Doyle-Price said the identifiable cost of emergency measures put in place to address the NHS ransomware attack was £180,000.

The Business Continuity Institute has called for improved user education and cyber resilience after revealing that nearly two-thirds (64%) of global firms have experienced at least one cyber "disruption" in the past year. In its latest report on cyber resilience, it looked at 734 responses from 69 counties and reported that one in six had experienced at least 10 disruptions in the 12-month period.

Strategic shift needed

Despite this, many organisations are still not facing up to the scale of the problem. One that I was talking to recently about offering them free cyber awareness training told me to speak to the IT team, a symptom of the way in which this threat is misunderstood. It isn't the responsibility of the IT team – it's a "C suite" issue, one that has to be strategically grappled with at the highest level.

All organisations – including those in the public sector – must consider cyber security an organisational risk, not just something that sits with the IT department. To mitigate against this risk, it is essential they raise their awareness levels and commit to creating a cyber-secure, risk-averse culture.

The costs of a cyberattack can be extensive. Following a mass raid on personal data in 2015, TalkTalk was hit by a 4.4% drop in new customers in the home services market, a £400,000 compliance fine, £15m in lost revenues and $45m in "exceptional costs". Surely this is enough for any chief executive to take notice and put cyber security on the top table as a priority?

There needs to be more recognition that, when it comes to fraud and corruption, horizon scanning and prevention is always the better way. Investigations after the event are always so much more damaging and expensive.

It's not all doom and gloom though. In the UK, we have a new National Cyber Security Centre (NCSC), with a mandate to "make Britain confident, capable and resilient in a fast-moving digital world".

Over the course of its five-year plan, the NCSC will invest £1.9bn in defending systems and infrastructure, deterring adversaries and developing a whole society capability – from the biggest companies right down to the individual citizen. Its website ▶

'Cyber security is an organisational risk, not just something that sits with the IT department'

(www.ncsc.gov.uk) is user friendly, contains free advice and offers free e-learning.

Fortunately, the Local Government Association recognises the work to be done and we sit on a working group with it, the Cabinet Office, NCSC and others that are trying to improve the response, and coordinate a robust approach to cyber crime.

Buyers (and sellers) beware

Another area where there is a mismatch between the level of threat and organisational preparedness is in the increasing risk of procurement fraud. When we visit organisations with the results of our CFaCT surveys, we ask: what is your biggest fraud threat? They always reply "procurement fraud".

Yet, when we look at the data on what is being investigated, we find the actual investigations are into council tax or housing or social care fraud. Procurement fraud is a lot further down the list.

Why is this? There are indications it exists, but it is hard to detect and also to investigate. Audit trails are not always good and there is a reluctance to dig deep – for many reasons. Procurement fraud can cover many areas that are close to an organisation's sensitive points: insiders who may collude, bid rigging, cartels, kickbacks, price fixing and corruption. It is interesting that so little is reported when anecdotally we hear of so many cases.

Procurement fraud in the public sector isn't very different to that in the private sector. In most cases, it takes some careful planning on the fraudster's part. The potential consequences of this type of fraud are wide ranging, including the delivery of substandard goods that can result in health and safety issues, as well as reputational damage and financial losses. Fraud and falsification can result in an organisation giving its customers an inadequate service or fake goods.

Awareness and an understanding of the nature of procurement fraud is the precondition for preventing it. This can be lacking among procurement specialists as well as in the supplier market. It does not mean that risks are ignored, but that the focus is too often on the ability to deliver the project to time, cost and quality – with too little attention paid to the possibility of fraud and corruption. This creates an environment where procurement fraud can flourish.

In 2013, referring to procurement fraud, the National Fraud Authority called for "a consistent and comprehensive strategy involving all elements of a counter-fraud response including prevention, detection, disruption, investigation and sanction". We have yet to see it.

Corruption: rare or unreported?

Linked to procurement fraud, there can also be corruption. In December 2014 we saw the UK government's first anti-corruption plan published, which recommended setting up the Counter Fraud Centre. CIPFA established the centre, and provided tools and services as well as drafting *Fighting Fraud and Corruption Locally* and raising awareness of the plan itself. But we have that found that awareness of corruption, red flags and other activity is patchy.

In 2015 and 2016, low levels of corruption cases were reported by those who completed our survey. Does this mean there is less corruption or does it mean it is not reported?

Perhaps it is hard to detect in many organisations; in the past, we have seen that corruption may involve high-ranking officials.

Detecting it and having a remit to investigate takes bravery and strength of character on the part of junior officers – and confidence that they will have unfettered access to the information needed. This may not be the most inviting prospect.

Nevertheless, in 2016, we saw some promising activity. The UK Anti-Corruption Summit in May resulted in commitments from 43 countries, with the aim of making more open data sharing available to support corruption investigations. The UK anti-corruption strategy was due before the June general election. We await the publication of this and the activity that will hopefully follow.

Despite all the difficulties, counter-fraud and anti-corruption activity is now receiving much more attention in the UK. The first government counter-fraud standards were published this year and there is a huge appetite to create a counter-fraud profession. Together with the growing collaboration on counter-fraud hubs, this development will hopefully help turn the tide on counter-fraud activity – and give it the profile and respect it deserves. A place at the top table in every public sector organisation will make sure that counter-fraud's position, high up on the agenda, is always assured. ●

'It is interesting that so little procurement fraud is reported when anecdotally we hear of so many cases'

PROTECT AND SURVIVE

Do the right things

ESSAY

BY MARK CHEESEMAN

With fraud now the most commonly experienced criminal offence, all organisations need to assess their risks and be active in seeking it out

Mark Cheeseman
is deputy director, public sector fraud, at the Cabinet Office

THE RELEASE of the Office of National Statistics' Crime Survey for England and Wales in January 2017 served as a reminder that the threat we face from fraud is very real. As the ONS said: "When the CSEW started, fraud was not considered a significant threat and the internet had yet to be invented. Today's figures demonstrate how crime has changed, with fraud now the most commonly experienced offence."

For those of us working to protect public finances, we are all too aware of the threat that fraud poses. A scan through recent cases of fraud in the public sector shows us that it is found on a frequent basis and in a variety of forms. The public sector is doing a lot of work to fight fraud, but we should be restless in our approach to fraud, and always be considering if we could do more.

We are all well acquainted with instances of tax and welfare fraud, and frequently see examples in the news. However, less often discussed but just as important are the instances of fraud in the delivery of public services, in the procurement and the delivery of contracts, in the administration and delivery of grants and even internally within the public sector.

Fraud is a hidden crime. To a greater or lesser extent, fraudsters try to hide their activity. As with all hidden things, this means if we want to find fraud we have to look for it. The public sector is finding fraud, but the evidence suggests to us that there is a lot of fraud out there that is still to be discovered.

We will never find all the fraud that occurs. Even in areas where we invest heavily in looking for it, such as welfare and tax, the statistics show us that we do not find it all. However, we should aim to get better at both finding and preventing it. By finding fraud, we can acknowledge and better understand it and, only by understanding it, will we be able to fight it effectively.

Fraud damages the services that the public sector exists to deliver – the services that many depend upon. Fraud also drives up public spending as it means that the services that we deliver cost more than they should or could. It is the role of public servants to protect public services from fraud and to ensure that taxpayers' money is spent where it should be.

Setting standards

So, how do we go about finding and understanding fraud? Central government has produced a set of Counter Fraud Functional Standards. These detail the basics that an organisation should have in place. They were developed by fraud experts in the public sector, who consulted with experts from other sectors. They are:

- Have an accountable individual at board level
- Have a counter-fraud strategy
- Have a fraud risk assessment
- Have a fraud policy and response plan detailing where accountability for fraud lies within the organisation, its delivery chain and how the organisation reacts to potential instances of fraud
- Have an annual action plan that summarises key actions to improve capability, activity and resilience in that year

- Have outcome-based metrics summarising outcomes they are seeking to achieve that year. For organisations with "significant investment" in counter fraud or "significant estimated" fraud loss, these should include metrics with a financial impact
- Have well-established and documented reporting routes for staff, contractors and members of the public to report fraud suspicions, and a mechanism for recording these referrals and allegations
- Report identified loss from fraud and error, and associated recoveries
- Have agreed access to trained investigators who meet the agreed public sector skill standard
- Undertake activity to try to detect fraud in high-risk areas where little or nothing is known of fraud levels, including using loss measurement activity where appropriate
- Ensure all staff have access to fraud awareness training.

All organisations should be aware of these. Some of them are focused on understanding the nature of the fraud threat an organisation faces. To begin with:

- Have well-established and **documented reporting routes for staff, contractors and members of the public** to report fraud suspicions, and a mechanism for recording these referrals and allegations.

Well established reporting routes are essential. If people do not know where to report concerns, it reduces their inclination to tell anyone, which makes it likely that crucial intelligence will be lost.

However, it should be remembered that reporting lines are reactive. They only deal with what people find (and are inclined to report). To have a modern and more effective approach to dealing with fraud, we need to look actively at what might be happening.

The following two functional standards deal with this:

- Have a **fraud risk assessment**;
- Undertake **activity to try to detect fraud** in high-risk areas where little or nothing is known of fraud levels, including using loss measurement activity where suitable.

The most important of these is having a fraud risk assessment. A fraud risk assessment done well tells a business what the main risks of fraud are, and where they are likely to be. It can then be used to proactively target counter-fraud activity to try to halt fraud before it even begins.

Previously, there had been no one way of carrying out a fraud risk assessment, and limited guidance available on how they should look. In 2016, specialists in central government came together to unite all the research and best practice on fraud risk assessment and then to write a set of standards and guidance for carrying out fraud risk assessments. These are now being rolled out across central government.

It is important that public bodies have an understanding of what a fraud risk assessment is, and what it should look like. A fraud risk assessment is similar to other risk ▶

'A good fraud risk assessment acts as the fulcrum for how the business deals with the issue'

assessments, but focuses on what fraud could happen to the business (as opposed to other things that may impact the business negatively).

Good fraud risk assessments identify specific acts that may be undertaken by specific stakeholders. They then consider how the control framework limits these risks. Importantly, what the business is left with is a strong understanding of the residual risk it faces, despite the controls it has in place.

The more specific a business's understanding of the residual risk is, the better. For instance, it is much more helpful to know precisely what would have to happen for a fraud to occur than it is to have an assessment that finds residual risk is low with no specific rationale.

Good fraud risk assessments bring frontline and fraud experts together to identify ways that an organisation could be defrauded – even in ways that the business has not had allegations about or has identified itself before.

A good fraud risk assessment acts as the fulcrum for how the business then deals with fraud. A fraud risk assessment can be compared to the referrals of potential frauds that are received, to see whether they are in the highest risk areas. We can then ask questions such as:

- If I am not receiving referrals in a high-risk area, why?
  - Is it because the risk is not as high as we think?
  - Is it because the circumstances in that area mean that fraud has not happened yet?
  - Or is it because we do not have what we need in place to detect fraud in that area?

This can then direct proactive detection activity to find more fraud, in line with another functional standard (to actively try and detect fraud). This may be something technical (like the use of data analytics tools) or targeted, random sampling activity, or it may be targeting specific audit activity, with a clear remit to try and find instances of fraud.

A fraud risk assessment, aligned with the referrals an organisation receives, can be used to direct fraud prevention activity. If an organisation knows that there is a high risk of fraud in an area, and/or that referrals are increasing, then there is a good rationale to consider investment in fraud prevention measures.

Increasingly, organisations are using data and data analytics to detect, deter and prevent fraud. A fraud risk assessment can be a core part of doing this, as it directs where to use analytics and also, when residual risk is considered in depth, ensures those using analytics understand the limitations of those analytics.

Fraud risk assessment is a growing discipline, and we now have a clear set of standards and guidance in the public sector. It is likely that, over the coming years, more and more people working in counter fraud will be fraud risk experts who help their businesses understand what fraud risks they are facing and how best to deal with them. Increasingly, we will see training that will help give people the necessary skills to do this work.

Having a fraud risk assessment, and people with the right skills to do it, are key to an organisation having a modern, comprehensive response to fraud. Through having a fraud risk assessment, the counter-fraud lead can make board members aware of where they are most likely to suffer fraud and agree any investment or activity they consider necessary.

Culture change

A fraud risk assessment is pivotal to dealing with fraud, but an organisation's overall counter-fraud response is driven by its culture. A fraud risk assessment can play into this, by making all levels of the organisation aware of the frauds that may happen.

The organisation's leadership team can also set the tone by encouraging the detection of fraud and embracing fraud when it is found. Finding fraud can feel like a problem, but it is an opportunity. As the crime statistics indicate, fraud is the most common crime, so we should not think that our organisations have failed if someone has tried to defraud them. Rather, our counter fraud response has succeeded if we were aware it was possible to be defrauded in that way, a business decision has been taken that meant we were content with the residual risk, but we detected the fraud when (and if) it happened.

The route to good fraud management is to understand fraud, embrace finding it and then evaluate whether an investment in further controls is needed.

All of those working to reduce fraud, whether fraud specialists, frontline staff or the senior management and board, should be restless in their understanding of fraud, and whether their organisation can deal with it. They should be curious about how fraud works, and how their organisations could be defrauded. They should also embrace finding fraud, seeing it as an opportunity.

By doing this, we can protect public services, keep the cost of those services down, and help ensure that taxpayers' money is spent on those services rather than going to those who would harm them. ●

'We should not think that our organisations have failed if someone has tried to defraud them'

Designing out fraud

ESSAY

BY IAN O'DONNELL

Austerity has produced some unintended consequences, including local authorities upping their game when it comes to preventing and detecting fraud

Ian O'Donnell *is executive director of corporate resources at Ealing Council, and lead for the London Counter Fraud Hub*

HENRY VIII created Hyde Park in 1536 as a private hunting ground, stag hunting on horseback being one of his favourite recreations. He liked hunting so much that he spent fully one third of his adult life on horseback. The only time he would do business during the day was when he was listening to mass, and late at night after a few drinks – because, from five in the morning until nine at night, he went hunting.

Most of the great parks were created by monarchs in this way, as royal hunting chases, enclosed from the 15th century onwards. The unintended but beneficial consequence of this medieval policy is that everyone can now enjoy the magnificent royal parks, which have been preserved as green spaces in spite of the enormous demand for land to build upon in the ensuing years.

The government's obsession with austerity policy has some of the qualities of Henry's obsession with hunting: the pursuit has been utterly relentless and the benefit to the common folk has been questionable. A further similarity is that austerity, too, has an unintended beneficial consequence. The austerity regime was set in place to effect government policies to close the national budget deficit and reduce the role of the state in the economy. As has been well documented, councils bore the brunt of the funding cuts.

In addition, the cuts arrived at a time when population growth had combined with advances in medical technology to boost the demand for local authority care services to unprecedented levels. Local authorities found themselves caught in the jaws of declining funding and increasing demand.

To exacerbate matters, the digital revolution that so enormously transformed services and business models in the private sector had not yet arrived in the public sector, and people using local authority services found their expectations of being able to access council services and information at the touch of a button were not being met.

The response demanded by this crisis of funding, demand and expectation was wholesale and urgent change.

Local authorities began to formulate large-scale projects to transform how they delivered their services. They are still in the process of implementing that transformation.

A new focus on outcomes rather than outputs is enabling them to concentrate on what is important for their communities. Learning from the private sector, they are adopting a more commercial approach, and are busy digitising their services.

Instead of simply rationing care services to keep spending within available funding, local authorities are managing demand through early intervention, reablement and helping people to help themselves.

In undertaking this transformation, they are having to renegotiate their relationship with the community and change their internal culture.

Guarding the gates

Amid all of this change, you could be forgiven for thinking that the issue of fraud risk could easily be forgotten. Happily, the unintended but beneficial consequence of business transformation has been that opportunities to defraud the system due to business ▶

inefficiency are being removed. There are three main areas in which this is happening.

The first is in the gatekeeping of local authority services. To determine whether a customer qualifies to receive a service, it is necessary to establish both their identity and their entitlement. The automation of these processes enables local authorities to respond quickly, meeting customers' digital expectations. It also helps them act more effectively as gatekeepers, reducing demand and enabling councils to tailor services more precisely to meet need. Identity can be verified quickly and effectively by using third party and council data.

Entitlement can then be assessed, checking the information provided to support the application against other data sources and using analytics to confirm the relationships between entities. The outcome is that the right people get the right services.

A further consequence of these checks is that fraud is designed out. Gatekeeping for the purpose of better rationing is yielding the benefit of fraud prevention.

The second benefit has been due to the redesign of business processes. Local authorities, in seeking savings by automating processes formerly carried out manually, are removing opportunities for insider fraud. By improving those business processes as they are automated, councils are also removing the inefficiencies within the system that were previously exploited by external fraudsters.

For example, procurement is an area that has been vulnerable to insider as well as external fraud, for instance through cartels. E-procurement using third party software has generated large-scale savings for local authorities – in addition, it has also removed insider opportunities to tamper with or unfairly assess bids. The data captured through the use of e-procurement systems makes it more possible to detect any collusion between bidders.

The third area is collaboration. The London local authority emergency response to the terrible tragedy at Grenfell Tower, providing support and assistance to the overwhelmed Royal Borough of Kensington & Chelsea, shows that local authorities are capable of excellent collaboration. However, collaboration has traditionally been an area in which local authorities have been slow to pursue opportunities. This is now changing fast, as the benefits of shared services and shared data are being sought in the race to find efficiencies and balance budgets.

The commissioning of the London Counter Fraud Hub by London local authorities is a direct example. The hub, sponsored by London Councils and provided by CIPFA, combines data sharing with advanced analytics to provide state of the art fraud detection and prevention that delivers cashable savings on a large scale.

In *Fighting Fraud & Corruption Locally*, the counter-fraud strategy for local government published by CIPFA in 2016, collaboration and the use of technology were highlighted as two of seven areas on which to focus.

These aspects of the fight against fraud have now come to the fore – even though they were driven by local authorities transforming business to make savings and balance their budgets, rather than by good practice.

Funding cuts are forcing councils to redesign their services as never before. The challenge local authorities face in managing the risk of fraud is the very same one they face in delivering services. Designing out fraud is the same as designing good business processes that deliver the outcomes required and represent good value for money.

No room for complacency

It is not all good news, however. Local authorities still have a long way to go to deliver their transformation plans, and are nowhere near designing out most fraud risks.

Fraud losses remain very significant. Furthermore, change brings with it new risks, and local authorities are now finding that their dependence upon digital systems is rendering them more vulnerable to cyber fraud, and the exploitation of their data.

Fraudsters will always adapt and evolve their techniques to exploit opportunities. There is no room for complacency in the fight to protect the public purse.

Many of Henry VIII's values and policies do not sit well in modern times. However, he was an innovator on a grand scale. He brought about the schism with Rome that led to the establishment of the Church of England. He allowed the translation of the Bible into English, making it available to the common folk. He created the British Navy, remodelled taxation, promoted parliament and established the kingdom of Ireland.

Were he alive today, Henry would undoubtedly applaud the scale of ambition of local authorities engaged in transforming their services. His policy on the royal parks, however, might still leave something to be desired. ●

'Designing out fraud is the same thing as designing good business processes'

Calling out financial crime

ESSAY

BY ANTHONY HARBINSON

Fraud, bribery and corruption cause untold misery and hardship and destroy trust. Accountants can play a key role in tackling these crimes

Anthony Harbison *is chair of the Fighting Financial Crime Task Force and director of safer communities for the Northern Ireland Department of Justice*

I HAVE A REAL PROBLEM with the terms "economic crime" and "financial crime" and particularly with the overarching term "white collar crime". The fact is that, over the past 30 to 40 years, these forms of crime – which include fraud, money laundering and terrorist financing, as well as bribery and corruption – have grown enormously to become a global blight that challenges national governments and private industry alike.

So why do I have a problem with these terms?

It stems from the fact that they mask the true pain and suffering these crimes cause. They give the impression of the act being almost a "clean" or a "victimless" crime in which, although people lose money, no one gets seriously hurt. This fallacy is genuinely damaging. We should all be aware from news reports about recent scandals that fraud and corruption affect everything – from a family's ability to feed and clothe their children, to the credibility and reputation of governments, to the financial health of businesses and even their ability to survive.

These crimes cause untold pain, suffering and misery and, yes, even death. This is not just on an individual level but, in certain cases, on a national level.

Financial crimes such as bribery and corruption create not only a substantial threat to the economic development and stability of a society but can, in extreme cases, lead to massive infrastructure failures and the collapse of vital services, as crooked politicians and public leaders siphon off badly needed funding into private offshore bank accounts and foreign property.

These are global problems which the UN, the World Bank, and the G8 and G20 countries have recognised. They understand that such crimes not only present a substantial threat to the development of national economies but also endanger global financial stability and security. NGOs such as Transparency International have been highlighting the problems these crimes cause for many years. However, despite the hard work of these bodies, there is growing evidence that developed countries, including the UK, are becoming safe havens for corrupt individuals and their assets.

These crimes can also damage the countries to which the funds are passed. Where the proceeds of crime can be siphoned successfully through legitimate financial systems, in countries such as the UK, they can undermine the integrity of those systems. And trust in the integrity of a financial system is part of the bedrock of our economy and prosperity.

New powers

That is why the Criminal Finances Act 2017 is so important. It is the latest weapon in the law enforcement arsenal in the fight against corruption, organised crime and global terrorism. The act provides the police and other law enforcement agencies not only with new powers to tackle financial crimes such as money laundering, terrorist financing and tax evasion but also greater powers in respect of the proceeds of crime and civil recovery.

The new power that may have the greatest impact concerns Unexplained Wealth Orders. These will enable our law enforcement agencies to require a person who is suspected of involvement in or who has a close association with serious criminal activity to explain ▶

the origin of assets with a value greater than £50,000 that appear to be disproportionate to their known income.

Organised crime and terrorist financing recognise no borders and that is why foreign property is also included within the scope of the act. In addition, it will also see the creation of two corporate "failing to prevent" offences: the failure to prevent facilitation of UK tax evasion; and the failure to prevent facilitation of foreign tax evasion. These new offences will operate on similar lines to the Bribery Act 2010 corporate offence of failing to prevent bribery – a corporate body will be liable if a person associated with it commits the offence.

The act will also seek to facilitate joined-up reporting of suspicions of money laundering. Currently, within sectors that are seen as at risk of being used to facilitate money laundering and terrorist financing, there are 25 watchdogs, 22 of which are accountancy and legal services providers' professional bodies. The government therefore plans to launch an "overarching watchdog" – the Office for Professional Body Anti-Money Laundering Supervision. When it goes live in early 2018, OPBAS will sit within the Financial Conduct Authority and its role will be to help improve the overall standards of supervision and ensure supervisors and law enforcement work together more effectively.

Another key feature of the act is that it amends the Terrorism Act 2000 by enabling the making of disclosure orders in connection with investigations into terrorist financing offences. In many ways, terrorist groups act like any other organised criminal organisation. They need money to operate and they need an effective financial infrastructure to procure weapons, bribe corrupt officials, attract new members and so on.

While these organisations can raise funds by exploiting legitimate sources, such as the abuse of charities or businesses, and raise funds from supporters, they also engage in criminal activities such as extortion, blackmail, human trafficking, smuggling and controlling prostitution. Some may even be sponsored by sympathetic governments.

So global terrorist organisations, like organised crime gangs, have a complex network of financial specialists, including accountants, who manage funds from a wide variety of sources, use the most up-to-date systems and techniques to move funds between jurisdictions, and constantly look for weaknesses and loopholes within our systems.

Constant vigilance on the part of the regulated sector is therefore essential.

'There is growing evidence that developed countries, including the UK, are becoming safe havens for corrupt individuals and their assets'

Ethics in accountancy

While the volume and scope of such crimes has changed, what has not changed is the fact that accountants have the skills and ability to tackle this criminal sphere. Our focus on ethics within the accountancy profession plays an important part in guarding its reputation, and establishing trust and ethical leadership must be at the heart of what we do.

We all have a role in ensuring ethical culture and behaviour are ingrained in the organisations we work for and senior management in particular should lead by example, showing others exactly what is expected of them. These crimes are deadly serious, and

tackling them requires coordination, communication and collaboration within and between organisations. We cannot afford carelessness or complacency.

As professional accountants, we must always address clear public concerns. As gatekeepers of financial systems, we play a unique role in assisting and supporting the government in implementing necessary measures by: ensuring that emerging threats are recognised; continuing to remain educated about emerging risks in order to remain vigilant; monitoring and assessing technology-related business risks; and ensuring that we have the right tools and defences to mitigate and reduce risks. We must always report any suspicious activity to the authorities.

While we have a key role to play in combating financial and economic crime, we cannot do this work alone. Making sure that the gates to our legitimate economy are as strongly guarded as possible is a job for everyone, inside and outside our profession. However, we are perhaps the best-placed profession to do this because our radar is always tuned in to risk and due diligence. We face a complex challenge for governments, policy makers and business. Nor is the public sector immune from these threats.

The responsibilities under the Anti-Money Laundering and Counter Terrorist Finance framework are challenging. Full compliance with both the letter and spirit of the regime is an objective that finance professionals must continue to strive to achieve. But if we believe, as I do, that the accountancy profession is a champion of ethical business conduct, then we must see our role in this area in a positive light. Tackling corruption and crime – and calling it like it is – is, quite simply, the right thing to do.

Working together, we can make a difference.

‘Terrorist groups need an effective financial infrastructure to procure weapons, bribe corrupt officials and attract new members’

Being part of the solution

BY JULIO BACIO TERRACINO

What is the OECD doing to combat fraud and corruption globally? *PF Perspectives* asked its deputy head of public sector integrity for his views

Julio Bacio Terracino *is deputy head of public sector integrity at the Organisation for Economic Cooperation and Development*

Why does the OECD place such a focus on the role of public sector integrity in tackling fraud and corruption globally?

There is increasing evidence of the importance of public integrity as a key pillar of political, economic and social structures. By public integrity, we mean consistent adherence to shared ethical values, principles and norms that uphold public over private interests in the public sector.

Corruption, fraud or more generally a lack of public integrity, real or perceived, has led to the disenchantment with politics and the economy that is evident in many countries. If a lack of integrity is part of the problem, the opposite should be part of the solution. There cannot be prosperity without integrity.

So, at the OECD, we work with governments to design and implement policies that strengthen public sector integrity systems as an essential element of economic and social wellbeing.

How does the motivation for fraud and corruption vary between countries?

We have found that the motivation does not differ that much from country to country. The good news is that very few people are straightforward liars or cheats. Some are, of course, just as some are very honest and will always try do the right thing. But the majority of people fall somewhere between these two categories.

They are impacted on by their surroundings and the context in which they make decisions. If you dropped them into a very corrupt country tomorrow, they would pay the petty bribes just like everyone else. And, if you dropped them into a country where corruption was not the norm, they would not.

We need to address this when we design and implement anti-corruption interventions. We need to ask ourselves: what are the accepted norms in a particular place that promote these types of behaviour? And how can we use public policy to challenge them and guide the majority of people towards ethical decision making?

These are the questions OECD member countries are asking and this is why we talk about a culture of integrity. This can play out in the world of public policy in several ways.

For instance, at the OECD, we are exploring how to educate young people about norms and behaviours that promote integrity. We know that education plays a profound role in shaping the civic values of the next generation, and we need to leverage this. Countries that have begun to educate their youth in this way are seeing promising results, as students with more civic knowledge tend to be less accepting of corruption and rule-breaking behaviour. Right now, we are working with the anti-corruption body and the education ministry in Greece to identify how education in public integrity can equip the younger generation with tools to prevent corruption.

We have also recently launched an initiative on evidence-based integrity. This involves working with governments and businesses to develop experiments, collect data and test ideas on what motivates individuals to act ethically.

How can the counter fraud profession change public sector culture, for example when it comes to the vetting of staff?

In the public sector, changing culture is about directly or indirectly changing the behaviour of an organisation's human resources. There are a number of HR management issues that undermine a culture of integrity and are impediments to creating open cultures.

These include issues like a high level of politicisation, which leads to party loyalty rather than loyalty to public service. Or a lack of guidance and commitment to integrity issues from the leadership. Or a low performance culture, and a lack of training and professionalism.

To counter this, we need public sectors around the world to look at how to make integrity a mainstream part of HR management practice. For example, during recruitment, some government bodies – as is the case in Australia – set "ethical tests" to assess a candidate's ethical skills and attributes. Other practices include developing job descriptions with ethical considerations in mind, and providing integrity induction training and dilemma training for government employees.

What is the best way for the public sector globally to maintain robust ethical relations with the private sector?

More is needed to ensure that interactions between public officials and the private sector uphold public integrity. Of course, the public sector must set standards internally and communicate them to external partners, but this is not solely the responsibility of the public sector. The private sector is responsible for respecting them too.

External communication by the public sector on its codes of conduct and ethical values can be an effective tool to inform users and providers about expected ethical conduct. A growing trend in OECD member countries is to communicate the values and ethics that public officials must adhere to throughout the private sector. In some countries, such as Canada, the code of conduct for procurement applies to both officials and suppliers, and suppliers are made aware of their required conduct. The UK government requires government suppliers to adhere to the "seven principles of public life", which are communicated via industry forums as well as guidance documents.

Knowing about these standards is the first step. The second and more difficult one is creating a culture of integrity within the private sector that respects them. This needs to go beyond mere compliance with expected laws, and must focus on creating a culture that discourages employees from breaking the rules. Much like with the public sector, it involves making integrity part of mainstream human resource management. For example, this could include using performance measurement and bonuses to encourage ethical behaviour, rather than creating pressures that encourage employees to cut corners. It also involves setting the ethical tone at the top, and ensuring the behaviour of a company's leadership is aligned with its code of conduct.

At the interface between the public and private sectors, it is of course vital to ensure that no one is requesting or offering bribes. But it also touches on other areas, like gifts and ▶

'There is a need to go beyond mere compliance to focus on creating a culture that discourages employees from breaking the rules'

hospitality, which are issues many countries are still dealing with. While accepting a sandwich lunch or promotional calendar is very unlikely to influence or be perceived as influencing a public official, it is not difficult to find examples of the private sector giving [more valuable] gifts such as entertainment or electronic equipment to public officials.

This sort of behaviour is detrimental to public integrity and there needs to be a clear understanding and commitment on behalf of both parties to refrain from such actions.

How can we encourage whistleblowing on fraud and corruption when so many cases end up with whistleblowers being publicly named?

Whistleblowing does indeed remain rare, but I would say this is not only because many of those who do it end up being named. True, retaliation against whistleblowers in the form of harassment, discrimination and career ostracism is, unfortunately, quite common. However, the main reason why people do not report acts of corruption is not the fear of retaliation but the belief that once they report a case nothing will happen.

It is mostly this loss of faith in the system that prevents people from coming forward and reporting acts of corruption. Additionally, negative connotations and perceptions in society around whistleblowing are perhaps an even greater obstacle.

For this reason, the surge in whistleblower protection legislation in many countries in recent years is welcome, but it is not enough. Much more attention should be paid to the "softer" aspects of whistleblowing, such as raising awareness about its importance, and communicating messages about the way whistleblowing contributes to an organisation or society.

Policies targeting the negative associations related to whistleblowing are necessary to make the cultural change that legal protection alone will not manage to accomplish. Without this key aspect, which is usually forgotten, we won't be able to effectively encourage whistleblowing on corruption.

What challenges do different countries and sectors have in common when it comes to combating fraud and corruption?

The challenges are not nearly as different as one might think. Of course, every country and sector is unique, and each has certain attributes that influence how they respond. But, across the board, everyone is dealing with the issues of entrenched norms and practices that undermine integrity. Some face this on a larger scale than others, but no country is immune to corruption.

What's interesting is that one of the main challenges we face is from the anti-corruption movement itself and its tendency to emphasise "flashy fixes" at the expense of duller, more long-term solutions.

An example is the overemphasis on open government. Obviously, opening up the government is necessary, and there are cases where government openness has enabled citizens to bring to light and punish corrupt behaviour.

But we need to be careful here: open government does not automatically motivate citizens to play an accountability role.

In fact, there is evidence that the level of openness in government does not strongly correlate with reduced perceptions of corruption, Other factors, such as the level of a country's administration and development, or the extent to which accountability mechanisms exist, must be taken into account. In settings where corruption is the norm, increased transparency may in fact give rise to resignation and withdrawal from political life.

Other research has found no significant relationship between freedom of information acts and reduced levels of public sector corruption. FOI acts don't operate in a vacuum – their impact is determined by the quality of a country's institutions, and their interaction with them. In the face of this, we at the OECD are working with countries to leverage the more "boring" but fundamental and sustainable solutions to preventing corruption. ●

'The loss of faith in the system prevents people from coming forward and reporting acts of corruption'


FUTURE
WATCH

Getting personal

ESSAY

BY ANDREW ROSE

In an era of increased data sharing, how can public sector organisations minimise the risks to individuals and organisations?

Andrew Rose *is public sector senior policy officer at the Information Commissioner's Office*

THERE'S A NEW LAW COMING into force next May that all those working in public finance and thinking about measures to counter public sector fraud should be keenly aware of.

Everyone whose job involves handling personal data, such as employee details, has a responsibility to keep that information secure and to ensure that individuals' rights are respected.

That's already the position under the Data Protection Act. However, from May 2018, this legislation will be replaced by data protection reforms including the General Data Protection Regulation (GDPR), an EU regulation that will apply throughout the UK. The government has confirmed that the UK's decision to leave the EU will not affect the GDPR coming into effect, and is introducing measures related to this and wider reforms in a data protection bill.

The GDPR is an evolution of legislation that will strengthen the accountability of organisations handling personal information, enhance consumer rights and give people greater control over their own data.

It is at its root a modernisation of the law. Many will agree that reform is long overdue. The world has changed a lot since the Data Protection Act came into force, in terms of not only technology but also business models, and people's attitudes to their data and expectations that their information is properly looked after. The law needed to change too.

New obligations

The GDPR will bring in new obligations for organisations. Public sector bodies will have to report data breaches that pose a risk to individuals to us at the Information Commissioner's Office and, in some cases, to the individuals affected.

They will have to ensure that specific protections are in place for transferring data to countries that have not been listed by the European Commission as providing adequate protection, such as Japan and India.

The GDPR applies to controllers and processors alike, and it places specific legal obligations on both to keep records of personal data and processing activities. For the first time, processors will have significantly more legal liability if they are responsible for a breach. But this does not relieve controllers of their obligations where a processor is involved – the GDPR places clear obligations on controllers to ensure their contracts with processors comply with the GDPR.

Public rights

Another key change that organisations need to understand concerns new rights for the public.

Consumers and citizens will have stronger rights to be informed about how organisations use their personal data. They will have the right to request that personal data is deleted or removed if there's no compelling reason for an organisation to carry on processing it, and new rights around data portability and how they give consent.

Consent will need to be freely given, specific, informed and unambiguous, and organisations will need to be able to prove they have it if they rely on it for processing data. A pre-ticked box will not count as giving valid consent. Where public sector organisations rely on consent to legitimise their processing, it is important to review this to ensure they meet the stronger test required under GDPR or find a different condition.

These legal reforms will increase regulatory powers, with powers to issue bigger fines for getting it wrong. If an organisation cannot demonstrate that good data protection is a cornerstone of its policy and practices, it could attract enforcement action that may damage both its public reputation and bank balance.

That makes data protection a boardroom issue.

But there's a carrot here as well as a stick and, as the UK regulator enforcing data protection law, we at the ICO actually prefer the carrot.

There is some scaremongering around, with suggestions that we'll be making early examples of organisations for minor infringements – or that maximum fines will become the norm.

The ICO's commitment is to guiding, advising and educating organisations on how to comply with the law. This will not change under the GDPR.

While it is vital that organisations are prepared to comply, they can also prosper in the new regulatory landscape. The organisations that thrive in the changing environment will be the those that look at the handling of personal information with a mindset that appreciates what citizens want and expect.

That means moving away from looking at data protection as a compliance issue to making a commitment to manage data sensitively and ethically.

It's also an opportunity to have a direct impact on public trust. Trust builds reputation, and both can be easily lost when people discover you haven't been completely honest about how you are using their information.

Our top tips for different areas are set out below.

Accountability

Having access to people's personal information means organisations have to act with great responsibility.

At the centre of the GDPR is the concept of broader and deeper accountability for an organisation's handling of personal data. The GDPR brings into UK law a trend that we've seen in other parts of the world – a demand that organisations understand and mitigate the risks that they create for others in exchange for using a person's data. It's about a framework that should be used to build a culture of data protection that pervades an entire organisation.

Public sector bodies need to implement technical and organisational measures that ensure and demonstrate compliance with the legislation. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies. ▶

'If an organisation cannot demonstrate that good data protection is a cornerstone of its policy and practices, it could attract enforcement action'

Privacy impact assessments

Another core component of the GDPR is the concept of data protection by design and default.

One very important measure that shows if an organisation has considered and integrated data protection by design into processing activities is the data protection impact assessment (DPIA); these are currently known as privacy impact assessments (PIAs). This tool can help organisations comply with their data protection obligations and meet individuals' expectations of privacy by identifying and mitigating against risks to this.

An effective DPIA will allow an organisation to identify and fix problems at an early stage of any new project or development, reducing the associated costs and damage to reputation which might otherwise occur.

That means organisations need to be thinking about privacy implications and data protection from the very start of projects or developments.

One of the standout findings from a recent ICO survey was that, although the majority of local authorities carry out PIAs, 34% do not. Under the GDPR, good practice tools – tools that the ICO has championed for a long time, such as privacy impact assessments and privacy by design – are now legally required in certain circumstances.

Staff knowledge is power

It's vital that staff keep data protection in mind – and this will be the case more than ever when the GDPR comes into force. Embracing a culture where PIAs are routinely used is one aspect of this.

In addition, public sector organisations need to ensure they have the right specialist staff in place. The GDPR requires that all public authorities appoint a data protection officer – a quarter of councils have told us they don't currently have one. The data protection officer's duties will include awareness raising and ensuring that staff who process personal data receive appropriate training.

Lack of staff awareness and understanding of data protection is behind many of the security incidents our enforcement teams see in the public sector and has led to many of the fines we have imposed to date.

Our survey found that 18% of councils do not provide mandatory data protection training to employees processing personal data; this will be a key area for data protection officers to address.

Help from the ICO

Our main aim is to help organisations get it right when it comes to using personal data – and that includes preparing for GDPR.

There's a wealth of material on our website to help, including pages dedicated to data protection law reform, including the GDPR. The address is ico.org.uk/dpreform.

The website also include our priorities in the coming months and how they will affect

'Lack of staff understanding of data protection is behind many of the security incidents in the public sector and has led to many fines'

you. Guidance on the GDPR includes an overview of the reforms, 12 steps to take now, a checklist to help you get ready and, importantly, messages for the boardroom.

The same section includes the Law Enforcement Directive, which covers the processing of personal data to prevent crime, and the movement of such data. There is also a section with useful links and further reading.

Stay in touch

If you want to stay updated on new guidance, our e-newsletter (http://bit.ly/2rxJiOL) is a good place to start. As well as the guidance on our website, businesses can also call our helpline on 0303 123 1113 or make use of our live chat service (http://bit.ly/2xP2vdN).

'Organisations need to be thinking about privacy implications and data protection from the very start of projects or developments'

Safety at work

ESSAY

BY GARY WALKER

Public sector fraud and corruption need to be exposed. So how do we take the fear out of whistleblowing?

Gary Walker *is an independent adviser on governance, a trustee of Public Concern at Work, and a former NHS chief executive and whistleblower*

IN 2013, I GAVE a presentation to a meeting of all the chairs of risk and audit committees from every government department, organised by the Treasury. We discussed what could go wrong if whistleblowers were ignored and how to create the right culture for employees to speak up about fraud, corruption, breaches of health and safety, and other unlawful activities without fear of reprisal. One of the chairs remarked that the greatest risk they faced was from the unlawful actions of their own employees.

Most organisations now manage business risk very effectively, including: focusing on risk management, controls assurance, fraud prevention, compliance with the law and regulatory standards, and securing information systems.

But, even with the most elaborate systems, unlawful activities persist. The NHS, for example, like all public sector bodies, has well-developed assurance, prevention, risk and compliance systems, yet estimates for NHS fraud are put as high as £7bn annually. It should be noted that the Department of Health believes it is significantly less than that.

Reporting and compliance systems, while necessary, are just one dimension of organisational assurance.

A worldwide study in 40 countries showed that 40% of the 5,400 firms studied had suffered from serious economic crimes resulting in an average of over $3m (£2.3m) each in losses. A significant proportion of these crimes – 43% – were exposed by whistleblowers.

What we typically find within organisations is that whistleblowing policies are weak or legally flawed, are not adhered to – and there is no real commitment from senior leaders to develop top-level reporting and open cultures to make them effective.

Organisations need to focus much more on getting their culture right so that all employees feel confident they can talk openly about any concerns they have and can report wrongdoing without fear of adverse consequences for them.

Good and bad practice

I was a member of a commission into whistleblowing led by a former court of appeal judge, Sir Anthony Hooper. We examined over 1,000 whistleblowing cases and evidence from employers, regulators, MPs and campaigning organisations. We made 25 recommendations and produced the Whistleblowing Code, which has been widely adopted across all sectors. We were sponsored by Public Concern at Work, the leading authority on whistleblowing in the UK, which this year also produced a detailed best practice guide on how to implement effective whistleblowing arrangements.

During the evidence gathering for the commission, we found that more than half (52%) of employees who had observed wrongdoing did not report it. From our research, one possible reason for that is that 74% of whistleblowers said nothing is done about the wrongdoing.

Another, more devastating reason is that when employers do respond, they take disciplinary action or demote the whistleblower (19%) or dismiss them (15%).

We know from almost every major scandal, case of patient harm or disaster – from Libor to Winterbourne View to Zeebrugge – that there was a whistleblower who was ignored, or action was taken against them.

Today, taking the wrong action against whistleblowers can have serious consequences for an organisation, its balance sheet and its directors.

One of the highest profile whistleblowing cases this year concerned Barclays Bank, where chief executive Jes Staley made repeated attempts to uncover the identity of two whistleblowers. By law, whistleblowers have the right to anonymity. Staley admitted earlier this year that he had made "a mistake".

His actions resulted in formal investigations into the bank and into Staley's conduct by the Financial Conduct Authority and the Bank of England's Prudential Regulation Authority. This could result in a fine for Barclays and the regulators could force Staley from his job.

Financial consequences

The financial cost alone of not addressing whistleblowers' concerns can be significant. If an employee seeks legal redress, fees and uncapped penalties can run into many millions of pounds. Most disputes are settled out of court but the financial cost can still be damaging, especially to public service budgets, which have never been more stretched.

Often there are calls from whistleblowing lobby groups to move to a US-style financial compensation model. These can result in successful claims in the hundreds of millions of dollars. While many resist this incentive model, it may only be a matter of time, and just take a few more high-profile scandals, before this becomes a desired option for legislators.

In response to the Mid Staffordshire Hospitals NHS Foundation Trust inquiry, the government imposed a duty on healthcare organisations, known as the duty of candour, to be open and transparent about when things go wrong.

There has been no move yet to place a general duty on employees to report wrongdoing but that may follow if organisations do not respond effectively to concerns from employees. Some professional bodies have placed a duty on their members to report wrongdoing as part of their conduct requirements.

One conflicting feature of whistleblowing is that, when it works well, almost no one knows about it. Rarely do organisations or individuals want to openly admit there have been any problems, especially if they were unlawful. However, culture will never change if organisations, businesses, the media and the public cannot accept that things go wrong in human systems, and that the focus should be on what is being done rather than fixating on what went wrong or who is to blame.

When I ran NHS hospitals, I would meet patients if their care had been substandard or they had come to harm. Most of these events would be a result of human or system error and, once we explained that we'd taken steps to learn and to reduce the risk of error, every patient was satisfied. Where we uncovered fraud, such as falsification of overtime, we dealt with it quickly and fairly, and spoke openly about the learning from all events.

The questions we should all ask ourselves is: would you get on a train managed by a company that doesn't respond to concerns from the drivers or engineers about unsafe brakes? Would you want to be cared for in a hospital that victimises nurses for raising ▶

'Would you get on a train managed by a company that doesn't respond to concerns from the drivers or engineers about unsafe brakes?'

concerns about a lack of staff? Would you want your safety protected by police services that dismiss staff for raising concerns about corruption?

Organisational culture and wrongdoing are inextricably connected. Organisations with the right culture, which take appropriate and decisive action, will experience less damage to their reputation, their employees, customers and finances.

When concerns are raised, these must immediately be investigated by someone who is independent and does not have a conflict of interest around the issues raised. No one should fear reprisals, even if they were misguided in their concerns. Indeed, the law protects whistleblowers provided they genuinely believe they are right.

Organisations must be as open about failure as they are about success, and must talk about whistleblowing, fraud, corruption, and breaches of health and safety and the law as candidly as possible. There should no parts of the organisation, services or actions of any employee, including directors, that are off limits.

Apart from being morally desirable, the global evidence is that it is financially prudent to encourage whistleblowing.

Next year, the Public Interest Disclosure Act 1998 – the UK's whistleblowing law – is 20 years old. It continues to do its best to protect the public and employees and to indirectly protect organisations from failure. But we shouldn't really need a law to be able to speak freely about wrongdoing. Speaking up should be as normal as saying hello.

'The financial cost alone of not addressing whistleblowers' concerns can be significant'

Take back control

ESSAY

BY KATY WOROBEC

Scammers are constantly devising new ways to steal money and data. Public sector organisations and their staff need to keep up to speed with the risks

Katy Worobec *is head of fraud and financial crime prevention, cyber and data sharing at UK Finance*

EVERY DAY, INDIVIDUALS AND ORGANISATIONS across the country are targeted by sophisticated scammers. With deception scams on the rise, knowing how to protect yourself and your staff from becoming victims of fraud is more important than ever.

There has been some progress on this front. Banks, for example, take fraud seriously and have worked hard to put robust security systems in place, resulting in £6.40 in every £10 of attempted fraud being stopped.

Unfortunately, this has led to fraudsters adopting different tactics, and targeting potential victims more directly. As a result, cases of financial fraud are on the rise.

Despite the dangers posed by these criminals, there is a lot of evidence that the majority of organisations are not taking steps to protect themselves adequately when it comes to fraud.

Stop and think

Recent research suggests that almost half of business leaders do not believe they will fall victim to financial scammers. More worryingly, most admit they have never heard of common scamming tactics, such as when fraudsters impersonate a chief executive or another senior person in the organisation to extract a financial payment.

The research was carried out on behalf of Take Five to Stop Fraud (https://takefive-stopfraud.org.uk), a national campaign designed to combat financial fraud in the UK. Backed by the UK's major banks and key financial services providers, Take Five is designed to help put the public and providers back in control with straightforward advice to help prevent fraud. This includes reminding everyone that it pays to stop and think.

This is relevant when it comes to combating fraud against organisations, in both the private and public sectors. Scammers often work on the principle that those they target will assume the request or instruction is coming from a trusted source – such as a senior manager – and automatically make a payment or share classified details without fully questioning what they are being asked to do.

Too often, I hear stories of fraudsters using spoof emails to impersonate a senior member of staff to deceive employees into transferring money, or pose as a regular supplier to a company or organisation in order to request a change in bank account details.

Sadly, these scams are easy to fall for. All too frequently, they work – in many cases with ruinous consequences.

Everyone's business

In reality, organisations of all sizes and types can be affected. It is everyone's business to be much more vigilant when it comes to the tactics that fraudsters deploy.

Fraudsters target individuals through a variety of methods. The most common approaches we see are when fraudsters contact potential victims through email or text messages, often using the name of a well-known company, and asking them to click on a link to update their details.

Technology means fraudsters can send text messages which get linked to an existing ▸

thread. So it is important for people to be vigilant, and only click on a link or return a call if they are absolutely certain that the organisation which sent the message can be trusted.

Additionally, fraudsters will make approaches by phone. They may pretend to be from the victim's bank or the police, and tell them there has been fraudulent activity on their account and that they need to move their money to a safe account.

In reality, neither banks nor the police will ask people to do this, nor to tap their PIN into the phone or withdraw cash to give to them for safekeeping. Yet vulnerable members of the community, in particular, can easily fall prey to these scams.

Another approach used by fraudsters is to pose as an employee from an organisation such as a broadband provider, and offer to fix an issue with a computer or another service. Individuals, including employees, must always ensure they know exactly who they are talking to, and never give callers remote access to their computers.

In all instances, whether fraudsters are targeting individuals at home or at work, it is key to have the confidence to check whether they are who they say they are. Any genuine organisation will not mind if people call them back on a number they know to be correct.

Keep it simple

Meanwhile, there are some simple steps that should be taken to protect every type of organisation:

- Ensure all staff who process supplier invoices and who have the authority to change bank details are vigilant
- Any changes to supplier financial arrangements should always be verified with that supplier, using established contact details that are already held on file
- When a supplier invoice has been paid, it is good practice to inform that supplier of the payment made, including the account the payment was made into
- Check company or organisation bank statements carefully and make sure all suspicious debits are reported to the bank immediately
- Fraudsters conduct extensive online research to identify suppliers to particular companies and organisations. Consider whether it would benefit your company or organisation to remove this information from your website, as well as from other publicly available sources
- Do not leave bills lying around for others to look at and record all details of standing orders and direct debits
- Educating staff is key. Ensure everyone in the organisation, especially finance staff, is aware of these types of scams and make sure staff know how to challenge unusual requests. Consider putting in place a system that strengthens controls around the transfer of funds. This could include requiring approvals from two people apart from the person making the request to initiate a transfer.

Above all, it is vital to remember to Take Five – to pause and think – before responding to any requests to share financial details. By doing so, we can all play an active role in protecting the public at large from financial fraud.

'A majority of organisations are not taking steps to protect themselves adequately when it comes to fraud'

CIPFA The Chartered Institute of Public Finance & Accountancy

tackling fraud demands specialist skills

Knowing how to prevent, detect and recover fraud losses could make all the difference to your organisation and career

Our qualifications focus on:

- investigative skills
- raising fraud awareness
- creating an anti-fraud culture
- managing fraud risk
- preventing bribery and corruption.

Visit: **cipfa.org/counterfraudevents** or contact the team on **020 7543 5600.**

04/2017

Out of the shadows

This is the sixth in a series of *PF Perspectives*, produced by CIPFA and *Public Finance*. They are designed to stimulate discussion on key public finance and policy issues. These essays, by leading public sector practitioners and experts, examine the far-reaching implications of fraud for public sector organisations and discuss strategies to detect and counter it

The Chartered Institute of Public Finance and Accountancy is the professional body for people in public finance. Its members work throughout the public services and in audit agencies to make sure public money is effectively managed. It is the world's only professional accountancy body to specialise in public services
cipfa.org

Public Finance provides news, features and expert comment on current public finance and policy issues, through its monthly magazine *Public Finance* and its websites
publicfinance.co.uk
publicfinanceinternational.org