Risk control

Fraud

In partnership with

GALLAGHER BASSETT
GUIDE. GUARD. GO BEYOND.

Risk Management Partners
rmpartners.co.uk

Fraud

Introduction

For public sector organisations, every pound lost through fraudulent activity, is a pound less that is spent on essential front line service delivery to residents. That is why proactive steps are taken to safeguard against fraud from external sources.

However, we must not neglect the very real risk that defrauding could come from within.

Employers place great trust and confidence in their loyal workforces and can be blindsided by the signs that they could be breaching that confidence. The control framework for internal fraud needs to be as robust as that for external fraud.

The Cost of Employee Fraud

The employee fraud could range from small stationery items, to inflated expense claims and beyond to significant payroll fraud, involving a number of employees.

Data from Action Fraud showed that British businesses reported £88m of insider deception in 2017/18 – double the previous year – with the average loss rising to £62,000[1].

If this trend continues it will inevitably lead to a potential contraction of the insurance protection available and/or insurers looking for the introduction and enforcement of tighter audit controls.

Fraud from External Sources

The value of external fraud detected or prevented in 2018/19 across UK local authorities is estimated to be £253m. This figure equates to a reported 71,000 cases of fraud. The hot spot fraud areas are housing, disabled parking concession, business rates and council tax[2].

Such losses of course sit outside of the traditional insurance (crime) covers offered by insurers but serve nevertheless to highlight the propensity of society at large to commit to fraudulent activity.

There is bountiful support for local authorities on how to design and implement their fraud strategy; from Central Government, the National Audit Office, CIPFA and the Fraud Advisory Panel – to name a few.

Each local authority is responsible for establishing appropriate mechanisms to manage the risk of fraud within their own authority.

This includes policies, systems and processes and the focus is normally two-fold – reactive counter fraud work including investigations and sanctions and preventative fraud activity focussed on intelligence monitoring to detect fraud hotspots.

The success of the authorities' counter fraud strategy lies in how well supported it is from the most senior leaders of the organisation as well as how embedded it is throughout the organisation. In addition the discipline that comes with completing an insurer proposal form (if you are asked to) can also act as a powerful checklist of controls and procedures.

Fighting Fraud

The Fighting Fraud and Corruption Locally (FFCL) 2020 strategy has been developed by local authorities and counter fraud experts. This strategy is supported by CIPFA and is the definitive guide for council leaders, chief executives, finance directors and all those with governance responsibilities.

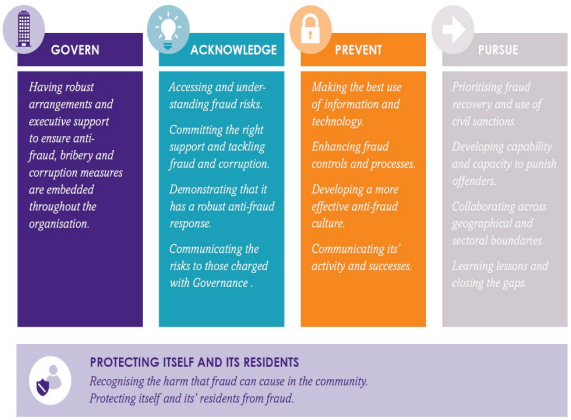
The most recent strategy has built on existing good practice across local government and includes recommendations for a more co-ordinated response to fighting fraud within local authorities on a local level. The strategy can be downloaded for free from the CIPFA website here: https://www.cipfa.org/services/counter-fraud-centre/fighting-fraud-and-corruption-locally

The strategy sets out a governance framework of pillars of activity for local authorities to concentrate their fraud management efforts on as well as tools to support implementation and case studies of successful fraudulent convictions[3].

[1] https://natwestbusinesshub.com/articles/12a16191-0482-966b-9b77-b46c5485c1d6

[2] https://www.cipfa.org/~/media/files/services/ccfc/cfact%20summary%20report%202019.pdf?la=en.

[3] https://www.cipfa.org/services/counter-fraud-centre/fighting-fraud-and-corruption-locally



For internal fraud prevention; public sector organisations should ensure they have a robust and effective internal control framework in place and that they proactively work to identify their potential hotspots and test their processes and procedures. Auditing, performance monitoring and well established risk reporting procedures will all help to strengthen internal fraud prevention.

Successful Prosecutions

Local authorities regularly publish successful fraud convictions they secure which highlights their zero-tolerance approach to fraudsters stealing from the public purse. There are cases where the fraud is perpetuated by individuals within the authority.

In London, seven housing benefit assessors were convicted after stealing more than £1m from three London authorities; Lambeth, Kingston and Barking & Dagenham. The employed assessors created false housing benefit claims and sent the funds to accounts they controlled themselves. The fraud spanned a period of 6 years. The crime ran deep, using council systems to generate council letters and to set up appointments for the fraudsters at the council. Following a three-month trial, the fraudsters were sentenced to prison for a total of 17 years.

In speaking of the crime, Ben Reid of the Crown Prosecution Service (CPS) said - 'These council-employed assessors were trusted to look after badly needed public money meant to help people find somewhere to live, Instead they corrupted the systems and sent over one million pounds to money launderers in the criminal underground[4].

COVID-19

Covid-19 has driven intense and rapid change in working practices with those who are compelled to work from home. It's proving to be a boom for cyber criminals however, who are capitalising on this period of unfamiliarity and uncertainty to catch people unaware[5].

QBE Europe have set out a list of their top tips for you to effectively manage your own cyber security:

Fraud Protection Guidance: *Take the Trouble to Double Check*

• Watch out for Scams

Organised crime has made a fortune from fraud, especially in the last five years. In commercial business, cybercrime **is** fraud. A large amount of this fraud is driven not by advanced cybercrime but by relatively simple scams. Users have come to rely on, and trust, technology and the internet so scammers are increasingly looking to take advantage of what are often low-trust systems, (such as email) to deceive their victims and commit fraud.

Every fraud starts with a communication. The principal method of scamming continues to be email. Whilst most government systems employ a range of security to block phishing and other scam emails, some do still get through. It is an unfortunate fact that attackers hijack the mailboxes of trusted third parties and use these to send scam messages to government employees and these may not be detected leaving the recipients as vulnerable as the senders.

Working from home also introduces further vulnerability where processes and technology which may have offered some safeguard against fraud will no longer be effective against attackers who are able to take advantage of the situation using the methods of attack described below.

As a result, it is vital that all communications are viewed through a lens of suspicion. If a message is unexpected or an unusual call to action and is requesting an immediate payment or inviting a file share or asking the recipient to follow a link, it may well be a scam. Confirm the validity of such messages with the sender and do not rush! The 'call to action' ploy is often a sign of malice and legitimate communicators will always be happy that you took the ***trouble to double*** check.

[4] https://www.localgov.co.uk/Council-employed-gang-convicted-of-1m-benefit-fraud/47085

[5] https://qbeeurope.com/resilience/top-tips-for-cyber-security-during-covid-19/

- **Methods of Attack**

Fraudsters have always sought to constantly evolve the methods they use to stay one step ahead of fraud prevention. Modern frauds are usually a combination of a few different, integrated scamming techniques as follows:

- **Phishing** by email or other method is rarely used in and of itself. It is part of the information gathering step and just the prelude to the attack. Essentially the aim of phishing is to obtain a victim's login credentials. Because users often set a common password for every system they access, it means that if attackers phish the credentials for one system, they are highly likely to be able use them on many other systems. The main targets include online (cloud) services such as Microsoft 365, Google Suite, Accounting systems, even online shopping as well as remote access to business systems. Frauds flow from this point because once the attackers have obtained unauthorised access to the systems used by key government staff or their suppliers, they are then able to use this as a staging post to launch monitoring and scamming to target key staff or third parties into revealing their credentials and finally into making fraudulent payments.
- **Social Engineering** by telephone, usually in combination with email. By faking the identity of someone who the victim believes, often by invoking in them a need for urgency through a call to action or by building trust in a series of apparently legitimate enquiries. This way, the fraudsters convince the victim to make or authorise a payment, bypass protective procedures or grant them access to their systems.
- **Fake Domains** by registering domains for fake websites and email addresses which are similar to those of legitimate organisations, fraudsters attempt to deceive victims into diverting expected payments to fraudulent beneficiary accounts. Usually this method includes the use of fake invoices.
- **Data Encryption & Data Theft** through unauthorised use of credentials stolen via phishing attacks. Over 60% of all ransomware attacks occur using stolen credentials to remotely access company networks.

  Data is then copied off, either manually or automatically, and ransomware dropped to encrypt the victim organisation's systems. Extortion demands then encourage fraudulent payment in return for often hollow promises to provide decryption keys or to prevent the release of stolen data.

<u>Vital protections against phishing, social engineering, and other fraud techniques</u>

Like any good approach to security, the most effective protection is achieved through a multi-layered solution. Then, if one defence fails, others will still prevent loss. Ensure all the following safeguards are acting in concert:

- Whilst technical solutions to detect and block phishing messages cannot be solely relied upon, they still provide a significant protection and are vital. Ensuring proper configuration of such technologies is key to their effectiveness so skilled technical specialists are needed.
- Staff awareness through fraud prevention training and regular phishing tests add another important control – risk-aware staff are the first line of defence. Raising risk awareness and restricting personal use of work technology can help limit exposure to some threats transmitted via social media, shopping channels, personal web-based email etc.
- Staff must use a unique strong password for each system they access. There are a range of ways to accomplish this using both manual, memorable techniques and/or with easy-to-use password manager apps. Staff should be reminded not to let anyone know their passwords.
- Strong authentication using one-time codes (often called two or multi-factor authentication) means that even if credentials are phished, the user accounts will remain resilient to attack.
- Domain name registration. Seek to register all close domain variants. If possible, choose a domain that is quite resilient to variation by making it as short as possible.
- As mentioned above, take the 'trouble to double'. Implement strict segregation between those who raise payments or arrange procurement and those who release payments or authorise expenditure.
- Implementing rigorous data backup regimes ensuring all data is saved in multiple locations which are not accessible to ransomware. Simple tape backup being one such option.
- Minimising authorised data access. Ensuring that users only have permissions to the data and applications needed for their specific job activity and that such permissions are revoked as soon as staff change role or leave the organisation. If accounts are compromised the losses are minimised.

- Inadvertent sharing of data with a fraudster mimicking a colleague, authority figure, or a trusted third party, can sometimes be the basis of extortion or manipulation into committing crime so absolute care is needed when handling or transferring data. Internal links should be used instead of emails and the need to send data externally, even if encrypted, should always be questioned. Double-check by having a colleague check the email and attachment to ensure they are correct.
- Strictly controlling administrative access to networks and applications. Administrators must use uniquely assigned accounts which are not used for normal business access.
- All accounting, payment and procurement systems activity should be logged. This includes online banking. Challenge your bank to ensure that they can provide a reliable audit trail of activity should an investigation be needed.

- **Protect the Most Vulnerable**

Modern fraudsters have well-developed processes which include gathering intelligence about their target victims. These criminals do not want to waste their time and so discovering and targeting those who control, or influence payments to, or by a government body, is a primary planning activity.

Those staff responsible for functions in finance/accounts, procurement and benefits are most at risk but even staff involved in areas involving refunds or repayments may also be targeted.

The first thing to do is to protect these staff by ensuring it is not easy for attackers to identify them specifically. This is not easy for government bodies who are used to promoting openness, but a good place to start is to ensure that contact information is non-specific and not published externally or internally unless it absolutely has to be, and even then, only to those with a specific need-to-know.

The third key protection is to implement a process of oversight; the 'double check'. No matter what the process of payment or procurement is, ensure that there is always a dual-control step. In payments, segregate those who can raise from those who can release. In procurement, ensure the use of effective processes of due diligence and authorisation split between those staff responsible.

- **Don't Forget the Inside Threat**

The insider threat of fraud is still very real for commercial, charitable and government authorities. Inside attacks may take place over an extended period and are often driven as much by an insider's personal problems as by malice or greed.

The best way to manage the risk of insider threat is again to take the trouble to double [check]. Where possible, strict due diligence checks should be performed on staff with financially sensitive roles, and warning signs for changed behaviours need to be watched out for. Failure to act in time (or at all) when there are known problems is not uncommon in many organisations – make sure supervision and performance reviews and any subsequent monitoring needed are working effectively.

Segregation of duties and strict system access controls should be used as the key operational barriers to prevent fraud. A layer of oversight above this should also mean that any anomalies would be swiftly detected.

Incident reporting and whistle blowing will also serve to enhance legitimate monitoring activities, but they need to be clear, accessible, and destigmatised to encourage staff to use those processes should they have any concerns. Line Managers have a critical enablement role in this respect and should actively promote responsible use of the Authority's reporting channels, leading by example.

- **Lead the Fight from the Top**

It is extremely rare for organisations that have adopted the fraud prevention advice given above to suffer from fraud. However, as Sun Tzu said, "Tactics without strategy is the noise before defeat"[6]. Organisations will be vulnerable if they do not support fraud prevention at the executive level.

That means appointing an Executive 'Fraud and Cyber Champion' who ensures the assignment of a suitable fraud prevention budget, the appointment of appropriately skilled staff and/or external expertise, and an effective governance framework to monitor and report on incidents and progress improvements.

[6] https://cio.economictimes.indiatimes.com/news/business-analytics/revealed-how-angel-broking-reconceived-its-business-model-for-digital-era/60933034

Summary

Fraudsters will try and exploit the vulnerability of local authorities whilst their attention is diverted and focussed on continuing to deliver front-line services with reduced capacity and restricted movements and/or operating capability.

Scams and frauds come in all shapes and sizes and all organisations are at risk. Local authorities always need to be alive to these, but the increased exposure that COVID-19 brings, means an even higher level of vigilance is needed so staff will need regular reminders on this count, particularly if working from home.

Support and Resources

To assess your current level of resilience, we recommend benchmarking against QBE's comprehensive risk controls provided in the following self-assessments:

- Fraud Prevention Questionnaire (part of QBE's Fraud Prevention Toolkit)
- Cyber Risk Profiler

These are available free of charge to QBE policyholders and are delivered online via QRisk. Both provide detailed guidance notes and a range of template documents, posters, checklists etc. to raise risk awareness and implement controls, and can be requested via qrisk.support@qbe.com

For a more bespoke approach with the added benefit of expert assistance, QBE Policyholders also qualify for discounted assessments with QBE partners STORM Guidance who contributed to the risk management advice in this guidance note. A consultant-guided risk review costs from £795, providing a jargon-free report advising on further controls needed to improve cyber resilience. This service can be requested direct from STORM - contact@stormguidance.com

Further information

For access to further RMP Resources you may find helpful in reducing your organisation's cost of risk, please access the RMP Resources or RMP Articles pages on our website. To join the debate follow us on our LinkedIn page.

Get in touch

For more information, please contact your broker, RMP risk control consultant or account director.

Risk Management Partners

The Walbrook Building
25 Walbrook
London EC4N 8AW

020 7204 1800
rmpartners.co.uk

FP809-2020