WHITE PAPER

FIGHTING INTERNAL FRAUD:

CLAMPING DOWN ON EMPLOYEE CRIME WITH ELECTRONIC DOCUMENT MANAGEMENT

Introduction

It is an unfortunate fact of life that not all employees are trustworthy and morally-minded. Even those employees that seem honest and loyal to the organisation can be tempted to carry-out fraud against their employer. Perhaps their financial circumstances have taken a turn for the worst, persuading them to take the risk, or maybe they have an underlying opportunistic streak which surfaces when their company's poor processes and controls allow fraudulent activities to go undetected.

Whatever the reasons why employees carry out 'internal fraud', whether it is over-claiming on expenses or carrying-out a more serious, organised crime, the fact is that it is costing businesses £billions every year and research suggests this is only going to get worse. The key is for organisations to accept that internal fraud happens and to get smart about fraud detection, monitoring and prevention.

The following white paper examines the real cost of internal fraud, discusses the 'typical' fraudster and then explains what steps can be taken to help prevent organisations from becoming victims. As technology is key to fraud prevention, the white paper will focus on how certain technologies, especially electronic document management systems, can help in the fight against employee fraud.

The real cost of employee fraud

Cifas, a not-for-profit company working to protect businesses, charities, public bodies and individuals from financial crime, explains that "internal fraud occurs when a member of staff dishonestly makes false representation, or wrongfully fails to disclose information, or abuses a position of trust for personal gain, or causes loss to others."

Cifas states that internal fraud attacks can range from being disorganised and opportunistic, purely for personal financial gain, such as inflating expenses, through to the more serious and organised activities by a criminal network.

However, despite the huge impact internal fraud is having on organisations' bottom lines, few organisations even admit that they have a fraud problem and so it is rarely tackled until it's too late. According to latest research by Gee and Button, 'The Financial Cost of Fraud 2015', organisations either deny that they have any fraud or plan only to react after fraud has taken place. As a result, fraud is now one of the great unreduced business costs.

The authors go on to state how important it is for the real costs of fraud losses to be calculated. They believe that it is only when the extent of fraud losses is known that these losses can be treated like any other business cost – something to be reduced and minimised.

The research has calculated that UK businesses and organisations are losing a phenomenal £98.6 billion to fraud and mistakes every year, which includes internal fraud. It also states that fraud and error losses in any organisation should currently be expected to be at least 3 per cent, probably almost 6 per cent and possibly more than 10 per cent. This level of loss should be ignored at an organistion's peril.

Worryingly, the costs of internal fraud are often much greater than an organisation realises. Of course, there are the direct losses due to the fraudulent act itself, however there are additional costs which are not always reported or which fail to be properly calculated and/or attributed to fraud.

According to Cifas in its 'Employee Fraudscape 2015', "the initial losses incurred by an organisation to internal fraud are wholly quantifiable, but there are other costs incurred – which relate to the actions that the organisation takes during the investigation of the fraud… Various staff members may be involved in the investigative procedure, which may mean that the organisation needs to recruit extra staff to cope with workload – another significant cost."

Cifas goes on to explain that there may also be costs associated with suspension and investigation and of course, regulators may impose penalties on the employers depending upon the nature of the fraudulent act itself.

Business fraud is a significant problem with Cifas reporting 276,993 recorded UK frauds in 2014 – a 25 per cent increase from 2013. This equates to 758 frauds every day! (Fraudscape: UK Fraud trends 2014). In its Fraudscape 2015 report, Cifas reveals that of the total number of frauds reported, a significant 56 per cent of fraudsters are on the inside. Insider fraud continues to be a growing problem with 751 confirmed cases of UK insider fraud recorded by Cifas Members in 2014; an increase of 18 per cent when compared with 2013.

Latest research by Kroll in its Global Fraud Report 2015-2016, paints an even more depressing Global picture, reporting that three-quarters of companies have experienced an incidence of fraud within the past year and of those, a shocking 81 per cent of the perpetrators have been insiders!

Who is the typical fraudster?

According to Kroll's Global research, within the past year, more than one in three victims (36 per cent) experienced fraud at the hands of a member of their own senior or middle management, 45 per cent at the hands of a junior employee, and for 23 per cent, the fraud resulted from the conduct of an agent or intermediary.

In terms of the profile of a typical fraudster, KMPG conducted research back in 2011 which remains valid today ('Who is the typical fraudster?', KPMG, June 2011). It identified the typical internal fraudster as being male, between 36 and 45 years old, commits fraud against his own employer, works in the finance function or in a finance-related role, holds a senior management position, has been employed by the company for more than 10 years and works in collusion with another perpetrator.

PWC's 'Global Economic Crime Survey 2014' echoes KMPG's findings, reporting that the typical internal fraudsters are middle-aged males with a college education or higher who have substantial tenure with the organisation.

It is often members of staff who are deemed the least likely to commit insider fraud who are presented with the greatest opportunities to do so. It appears that trusted, long-serving members of staff in senior positions are just as likely to commit internal fraud as more junior and seemingly less trustworthy members of staff. When an internal fraud takes place, especially when the fraudster is viewed as an unlikely criminal, it can shake an organisation to its core, resulting in damage to morale and reputation, as well as finances.

One of Japan's biggest corporate scandals has seen Toshiba's stock price fall by 40 per cent since May 2015 after it was revealed that three former presidents and two CFOs were involved in fraudulent accounting practices spanning seven years. An internal probe found construction costs on certain infrastructure-related projects had been underestimated and that losses from the construction work were "not recorded in a timely manner." Japanese regulators have recommended imposing a record fine of 7.37 billion yen ($60 million) on Toshiba, the largest ever in Japan for accounting-related violations.

Some notorious insider fraud cases from the past few years include the cases of cricket entrepreneur Sir Allen Stanford who orchestrated a fraudulent, multi-billion dollar investment scheme, and Bernard Madoff, the former chairman of the Nasdaq stock market, arrested for running a hedge fund which allegedly racked up a staggering $50bn (£33.5bn) of fraudulent losses – the biggest case of its kind. Finally, who could forget the Enron scandal which was brought about by all manner of financial cover-ups?

With organisations having so much at stake, it is vital that they implement watertight policies, processes and controls to mitigate the risks of internal fraud. These need to be able to identify, monitor, deter and ultimately, to help prevent fraud from ever taking place.

Types of employee fraud

There are many types of internal fraud, including the following:

- Theft of cash, physical assets or confidential information;
- Misuse of accounts;
- Procurement fraud;
- Payroll fraud;
- Financial accounting mis-statements;
- Fraudulent expense claims;
- False employment credentials; and
- Bribery and corruption.

The most common crimes, and the easiest ones to guard against, are opportunistic attempts by employees to metaphorically 'put their hand in the till' – for example, making up their own financial shortfalls by inflating their expenses or overtime claims, or purchasing personal goods through the company.

Expenses fiddles can seem harmless enough, but soon mount up. Common false claims include fictitious taxi rides; claims for un-receipted parking; adding mileage to journeys; and use of expenses claims to cover bar and restaurant bills.

The Kroll report (November 2015) also highlights the very real risk of supplier or procurement fraud with 17 per cent of companies surveyed being affected by vendor, supplier or procurement fraud over the past 12 months. Nearly half of companies (49 per cent) described themselves as vulnerable to this type of fraud. In addition, nine per cent of the organisations admitted being affected by internal financial fraud with 43 per cent feeling at risk of this taking place in their companies.

With an incredible four in five respondents (80 per cent) believing that their organisations have become more vulnerable to fraud in the past year, it's time for companies to take back control and to confront internal fraud head-on.

Taking back control

The main reason many organisations have been so vulnerable to employee fraud is their over-reliance on personal relationships and mutual trust, and their lack of visibility across finance management processes and systems. Too little insight into potentially dubious trends has by default given financially-stretched and easily-tempted members of staff a licence to push their luck and for line-managers to give the benefit of the doubt or even turn a blind eye to questionable transactions.

As the ongoing financial crisis has taken its toll on procurement budgets and expenses allowances, vigilance has increased however. With no slack in the system, companies have had no choice but to rein in allowances and clampdown on suspicious spending.

Turning to technology

The more systematically financial transactions and administrative processes are managed, and the more visibility there is across supporting systems, the more control organisations will have over their spending – and the more readily they will be able to spot and address potential problems.

One of the benefits of using technology to manage and protect against fraud is that it depersonalises the situation, removing the awkwardness involved if a manager suspects and accuses a team member, peer or even a superior of underhand practices.

There are several different approaches organisations can take to tackle employee fraud through technology. Some take a forensic approach, using sensitive analytics to identify unusual patterns of spending. Electronic procurement solutions, meanwhile, enable closer monitoring of purchasing, enforcing approvals and matching individual invoices and payments to purchase orders so that anomalies can't slip through the net – because everything is carefully accounted for. Such systems can be policed with a no-PO-no-payment approach, ensuring that no funds are issued without the requisite electronic 'paperwork'.

Automated expense management systems apply similar rigour, not only reducing the administration burden around expenses claims but also ensuring that approvals processes are followed through and that claims can be properly traced and monitored electronically.

How document management can help

As soon as records are being kept electronically and can be interrogated easily – i.e. because the content is centrally archived and readily searchable - companies inherently have much more control over the information contained in these documents, whether these are expenses claims, procurement records or processed invoices.

Having a clear line of sight across related documentation and being able to call it up instantly is becoming increasingly important from a financial auditing and regulatory compliance perspective too.

Whatever measures are taken to perform the actual fraud detection and analysis, the underlying platform enabling sophisticated monitoring of employee behaviour is electronic document management and imaging. As long as procurement, purchase orders, invoices and expense claims are handled in a largely manual way, there is a limit to how vigilant companies can be in monitoring potentially suspicious behaviour – because they have no way of readily accessing and comparing the information.

The good news is that this situation can be turned around easily and affordably. For minimal outlay and yet with a rapid return on investment, organisations can automate routine finance management processes so that the detail contained in traditional paper documents is scanned straight into core business systems - where it can be tallied with related records and shared with other systems and users.

Investing in document management to prevent fraud

Electronic document management systems, tightly integrated into organisations' accounting, enterprise resource planning (ERP) and HR systems, minimise the risk of fraud because documents such as invoices, purchase orders and personnel records are imaged (scanned and indexed) and then securely stored in an electronic archive.

These documents form a permanent record which cannot be destroyed or altered in any way, reducing the risk of an employee eliminating or manipulating evidence to cover their tracks - as Arthur Andersen staff did during the infamous Enron investigation in the US.

Following the 2001 scandal - in which $100bn revenue energy giant Enron was found to have sustained itself by means of institutional and systematic accounting fraud - Andersen's alleged complicity as an auditor came under intense scrutiny. In June 2002 the accounting firm was convicted of obstruction of justice for shredding documents related to its audit of Enron.

Document management systems impose strict levels of document access and maintain audit trails so that it is clear who approved what and when, further thwarting attempts to hide suspicious activity.

As noted above, one of the biggest problems for organisations in leaving themselves open to fraud has been the fact that there have been easy pickings for those desperate enough or easily tempted to harvest them. In the current climate, it is vital that staff are not provided with the means to easily commit fraud. Systems enabling electronic document management reduce the risk of fraudulent activity and should form part of organisations' cross-company security measures.

Choosing the right system

There are a number of fraud detection and prevention solutions on the market that come under the document management umbrella. Integrated with accounting/ERP and HR systems, these can become powerful tools in the fight against internal fraud.

The main component technologies include:

1. Document archiving technology. Such systems electronically scan or 'image' and store all documents, so that essential documents such as contracts, invoices and HR/payroll documents cannot be lost or destroyed. Once these documents are securely stored and backed up, they cannot be conveniently 'mislaid', shredded or burnt for the benefit of a fraudster (such destruction being the undoing of Arthur Andersen staff during the Enron scandal). Nor can documents be altered for an individual's own ends.

2. Electronic document form creation and delivery software (e.g. output management and automated mail). These systems replace the paper-based distribution of documents, a process that lacks a formal audit trail. Documents that are created using an electronic form designer and delivered by email can be stored in the central document archive so that there is a permanent record of which documents have been sent to whom and when. This transparency is a significant aid in unearthing any suspicious correspondence.

3. Purchase requisitioning software. This provides greater control over the procurement of goods, ensuring that any anomalies and maverick spending are spotted more easily. Ideally web-enabled, such solutions enable purchase orders to be raised, managed and authorised electronically, reducing administration costs, delivering greater procurement transparency and cutting rogue ordering of goods and services. Once approved the purchase order is generated or the requisition is automatically sent on for further levels of authorisation, depending on the controls put in place using the system's customisable business rules. All approved purchase orders can be printed, faxed or emailed directly to suppliers.

4. Electronic document authorisation software. This too can help prevent procurement fraud. Here, every invoice for payment can be routed for electronic authorisation, and there is an audit trail which records who has approved which invoice and when. This level of transparency makes it harder for staff to carry out fraudulent transactions.

5. Secure cheque printing solutions & special fraud-resistant stationery. These tools can be used to ensure that no bank or cheque details are pre-printed and that details are altered only by those authorised to do so. Stationery can be numbered too, making it easier to trace. In fact every document in an electronic archive has its own distinct 'electronic fingerprint', with any activity relating to that document being logged. As it is impossible to delete any of these activity logs, the attempts of even the most ardent hacker to cover their tracks would be detected.

   Not every organisation will have the same set-up or the same priorities, so it is important to look for a modular range of solutions that allow the required functionality to be mixed and matched, and blended with existing systems. Systems should ideally be easy to integrate with core business software, and scalable enough to expand as use grows. The right supplier will be able to advise on the right technology combination for the given environment, taking into account possible future requirements in addition to current needs.

Conclusion

Addressing potentially dubious activity can require delicate handling though, which places further emphasis on the need to use technology - to record the indisputable truth about what is going on as funds pass in and out of the company. Capturing everything systematically means no individual is seen to be singled out for special attention. Anomalies are simply highlighted as part of routine processes, because there is much more visibility in and across core business systems. For anyone involved in malpractice it means there is no longer anywhere to hide. For the business confronting the problem, there is detailed evidence of what went awry, when and in whose hands.

Prevention is far more effective than cure. Once staff are aware of the tighter controls this is likely to *deter* rogue activity, because the chances of being caught red-handed are so high.

Given the fairly modest investment required to automate associated finance processes, and the additional benefits as related business activities are streamlined and archiving, backup and auditing are automated, the barriers to adopting document management solutions are negligible. Easy integration with existing business processes and systems, and rapid payback in the form of considerable associated cost and time savings as well as reduced vulnerability to internal fraud, make for a robust business case.

Document management represents a solid investment to help prevent fraud. Given the potential damage to an organisation's bottom line, as well as its reputation, if it falls prey to malicious activity, it makes for a prudent business decision. With a further increase in corporate fraud expected in the UK, there is no time like the present to spend a little to save a lot.

Sources & resources

A short guide to fraud risk (Gower Publishing, March 2010) http://www.gowerpublishing.com/pdf/SamplePages/Short_Guide_to_Fraud_Risk_Ch1.pdf

CIFAS figures shed new light on insider fraud dangers (CIFAS, August 2012): http://www.cifas.org.uk/staff_fraud_augtwelve

Home Office Annual Fraud Indicator (National Fraud Authority, March 2012): http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/annual-fraud-indicator/annual-fraud-indicator-2012?view=Binary

Global Economic Crime Survey – UK report, (PwC, 2011): www.pwc.co.uk/eng/publications/global-economic-crime-survey-2011-uk-report.html

Kroll Advisory Solutions' Global Fraud Report (in cooperation with the Economist Intelligence Unit, 2012): www.krollconsulting.com/insights-reports/global-fraud-reports

Tackling Employee Fraud (Personnel Today, October 2012): http://www.personneltoday.com/Articles/25/10/2012/58931/Tackling-employee-fraud.htm

Who is the typical fraudster? (KPMG, June 2011): http://www.kpmg.com/uk/en/issuesandinsights/articlespublications/pages/who-typical-fraudster.aspx

News article: Fraud trial jury for former UBS trader selected (Reuters, September 2012): http://www.reuters.com/article/2012/09/10/us-ubs-trial-idUSBRE8890BO20120910

News article: PFG founder Wasendorf arrested in fraud case (CNN Money, July 2012) http://money.cnn.com/2012/07/13/investing/wasendorf_pfg/index.htm

News article: Expenses fraud considered among the more serious workplace crimes (Freshbusinessthinking.com, June 2012) http://www.freshbusinessthinking.com/news.php?NID=14419&Title=Expenses+fraud+considered+among+the+more+serious+workplace+crimes

News article: Taxi expense fraud rife as staff top up pay (People Management, October 2012) http://www.peoplemanagement.co.uk/pm/articles/2012/10/taxi-expense-fraud-rife-as-staff-top-up-pay.htm

Tackling staff fraud and dishonesty (Chartered Institute of Personnel and Development Guide) http://www.cipd.co.uk/NR/rdonlyres/710B0AB0-ED44-4BD7-A527-B9AC29B28343/0/empfraud.pdf

News article: Procurement fraud costs public sector £2.3 billion (Supplymanagement.com, April 2012): http://www.supplymanagement.com/news/2012/procurement-fraud-costs-public-sector-23-billion/

News article: An expensive problem for UK businesses (Professional Manager, March 2012) http://professionalmanager.co.uk/debate/3176/an-expensive-problem-for-uk-businesses/

News article: Staff expense fiddling tops 3.5 billion (HR Magazine, May 2010)
http://www.hrmagazine.co.uk/hro/news/1017900/staff-expense-fiddling-tops-35-billion

Enron: Who’s accountable? (Time Magazine, January 2002)
http://www.time.com/time/magazine/article/0,9171,1001636,00.html

Document management to catch a thief (CRN/ChannelWeb, July 2011):
http://www.channelweb.co.uk/crn-uk/analysis/2087743/document-management-catch-thief

The Financial Cost of Fraud 2015: What the latest data from around the world shows, Jim Gee and Professor Mark Button (2015) http://www.pkf.com/media/31640/PKF-The-financial-cost-of-fraud-2015.pdf

Employee Fraudscape 2015 (Cifas)
https://www.cifas.org.uk/secure/contentPORT/uploads/documents/External-Cifas-EmployeeFraudscape2015-onlineversion.pdf

Fraudscape: UK trends 2014 (Cifas)
https://www.cifas.org.uk/secure/contentPORT/uploads/documents/External-A5%20Fraudscape%20insert%20LOW%20RES.pdf

Toshiba shareholders sue over accounting (CFO, December 2015)

http://ww2.cfo.com/fraud/2015/12/toshiba-shareholders-sue-accounting/

Global economic crowd survey 2014 (Pwc, 2014)
http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/perpetrator.html

Corporate Fraud (CIMA, May 2009)
http://www.cimaglobal.com/documents/importeddocuments/cid_tg_corporate_fraud_may09.pdf.pdf

Business warned of enemy within on fraud and cyber crime (FT.com, November 2015)
http://www.ft.com/cms/s/0/22850590-906e-11e5-94e6- c5413829caa5.html#axzz3u81Eip5k

Kroll press release: ‘The threat within: Insider fraud on the rise’ (23 November 2015)
http://www.kroll.com/en-us/intelligence-center/press-releases/the-threat-within-insider-fraud-on-the-rise

About V1 Ltd

V1 Ltd ("V1"), is a global provider of electronic document management and imaging solutions that enable both public and private sector organisations to automate and simplify their processes.

V1's software integrates into all major accounting and enterprise resource planning (ERP) systems, enabling the automated delivery, storage, management and processing of documents. Thousands of organisations worldwide are using V1's software to streamline their business processes, cut costs, free-up administration time and reduce paper consumption while enjoying a typical payback of just six months.

V1 prides itself on its innovative solutions, personal and straightforward approach and dependable service.

V1 Ltd is an Advanced Computer Software Group company.

www.WeAreV1.com