Employee risk

Fat fingers.

Rogue traders.

Data theft.

Disgruntled employees.

There are many ways in which an individual's behaviour can threaten a company's operations and damage its reputation. We discuss the different types of employee risk that a company may face and consider how these risks can be managed.

What is employee risk?

Put simply, the term employee risk covers all the things that a company employee can do, whether intended or not, which can damage the employer's business in some way.

Employee risk in the treasury

The modern treasury is a highly complex work environment and the volumes of business transacted mean that when things do go wrong the impact will quickly become apparent, will sometimes be spectacular and can often be very costly. Human ingenuity is such that there is almost no limit to the types of damage that can be inflicted on an employer by an unhappy or misguided member of staff.

From the treasurer's perspective, then, addressing employee risk is an important part of the managerial challenge. Although all well-managed treasuries will have policies and procedures in place which set out in considerable detail how key elements of risk are to be managed by the business, it is particularly difficult to cover all the bases when it comes to dealing with employee risk. This is due to the sheer number of forms that it can take. In some respects it is this surprise element which makes it a more difficult category of risk to manage than either FX or interest rate risk.

Types of risk

Rogue trading

Whenever the subject of employee risk is mentioned, 'rogue trading' is usually the first topic which comes to mind.

Over the years there have been many high profile cases, usually in the banking industry, where a rogue trader has, through a combination of bravado, bad decision-making, lax controls and lack of managerial supervision, caused an employer to lose very large amounts of money. For example, in 2008 Société Générale's Jerome Kerviel lost his employer €4.9 billion.

Rogue trader cases are nearly always big news stories, and rightly so – rogue traders can cause serious reputational as well as financial damage to the company which employs them. They also tend to result in a lot of unwelcome scrutiny and questions from regulators.

Rogue trading is possibly the area of employee risk which concerns a treasurer the most, since it calls into question the treasurer's ability to manage the business. Apart from the financial damage to the firm there is an embarrassment factor – no senior treasury manager wants to be associated with, let alone implicated, when the big investigation takes place into what went wrong. It is certainly not good for the CV.

For the most part though, well-run treasuries should be able to rely on their internal controls, along with effective management supervision, to prevent rogue trading. It is nevertheless important that treasurers keep in close touch with the 'buzz' on the trading floor – this may help to identify an 'at risk' trader. The individual who thinks he or she is smarter than the market and has found a way to sidestep an internal control usually says or does something which will give some small clue to colleagues as to what's happening.

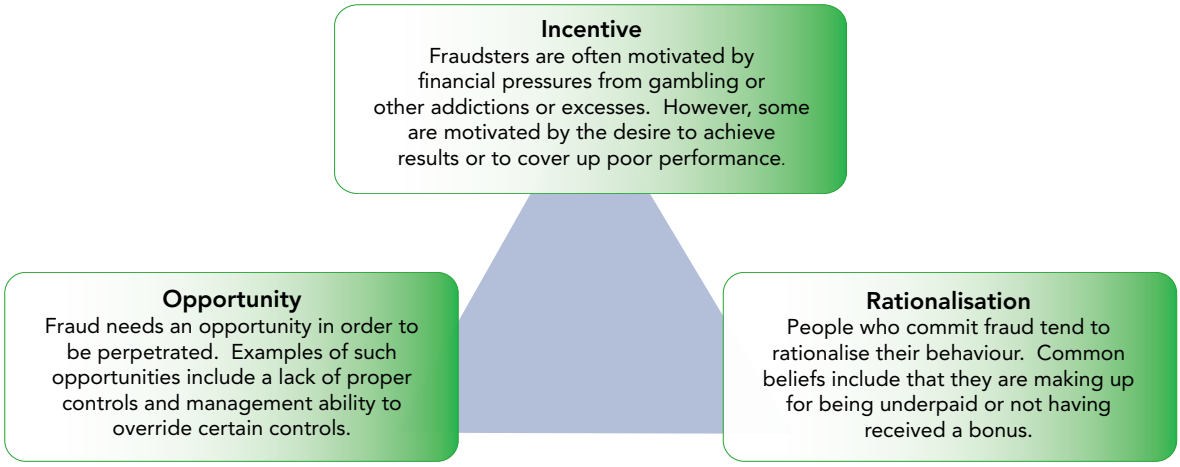
Employee fraud

Employee-related fraud risk is something that all treasurers have to be mindful of. In tough economic times, where people's job security may be under threat and where bonus levels are lower than in the good times, the potential for employee fraud tends to increase. Employees may well have made financial or lifestyle commitments in times of plenty, which they suddenly find themselves struggling to fulfil. Desperation to maintain a certain lifestyle regardless of an impending change in personal circumstances – combined with an opportunity to commit fraud – can lead people to cross the line.

Staff fraud comes in many forms, from straightforward theft, for example through submission of inflated expense claims, to opportunistic crimes where a procedural loophole or a weakness in the company's systems is exploited for personal gain.

The fraud triangle

Donald R Cressey developed the concept of the 'fraud triangle' in the 1950s as a way of understanding the psychology and driving factors behind fraud.



According to Cressey's theory, all three elements of the triangle – incentive, opportunity and rationalisation – need to be present before fraud can take place. Opportunity is generally acknowledged to be the area over which employees have the most control.

Analysis of 'insider' fraud cases by the Association of Certified Fraud Examiners in the US reveals some interesting insights. The 2010 edition of their Global Fraud Report states that:

- The typical fraud goes on for 18 months before it is detected.
- Insider fraud is more likely to be detected by a tip-off than by any other means.
- Smaller organisations are disproportionately targeted because they typically lack adequate controls.
- More than 85% of fraudsters have never previously been charged with or convicted of a fraud-related offence, making their activities even harder to detect.

According to KPMG's UK Fraud Barometer, 2009 saw 'a dramatic increase in serious employee fraud'. Losses totalled an estimated £567m, the highest level since the barometer began 22 years ago.

Theft of corporate data

The theft of confidential corporate data by employees is a sub-set of employee fraud, but it ranks as another big area of concern for treasurers. This type of fraud has the potential to inflict major reputational damage on the firm as well as damaging important client relationships.

In 2008 an employee of Countrywide Home Loans in California was found to have been downloading information on around 20,000 customers a week onto USB devices over a two year period. He sold each batch of customer information to a third party for $500. Clearly this was not good for Countrywide's business or for their reputation. The fraud could probably have been prevented if the company had had better monitoring controls in place over what information was being downloaded by employees onto external devices.

The sheer number of cases of corporate data theft reported in the media does seem to suggest that this type of fraud is particularly difficult to prevent. If employees need to have company data on their PCs, BlackBerrys and other portable devices in order to do their jobs effectively, it is inevitable that sooner or later a company laptop will be left on a train or a plane. Companies need to have policies and procedures in place to deal with data theft or data loss, both in terms of rendering the information useless to the finder and managing any negative PR fallout. No treasurer would wish to see details of major client trading positions and pricing, lists of staff bonuses or sensitive internal memos posted on the web for the whole world to see.

Human error

Despite all of the technology used in stock markets and company treasuries to check, analyse and if necessary block trades input by humans, errors still occur and these can prove very costly.

In 2005 a 'fat-finger' keyboard error by a junior employee on the dealing floor of Mizuho Securities in Japan ultimately led to the resignation of the Head of the Tokyo Stock Exchange (TSE). The TSE's trading system failed to block a sell order for 610,000 shares in a manpower recruitment firm at JPY 1 apiece – the trader had actually intended to sell one share in the firm at JPY 610,000. The firm only had 14,500 outstanding shares, so the sell order was over 40 times larger than this. Confidence in the TSE had been undermined by its failure to spot the erroneous trade and it was this which cost the TSE Head his job.

For Mizuho, which was forced to buy back the shares at a higher price, the incident cost the equivalent of three months' net profit. All end of year bonuses in the securities division were cancelled as a result.

The following year, a $50m trade was executed earlier than planned when a rugby ball landed on the keyboard of a Bank of America trader. The trade had been set up to execute when the trader pressed enter.

Mundane, yes, but still potentially damaging

While rogue traders, employee fraud cases and fat-finger errors tend to grab the headlines there are other types of employee risk which can also lead to serious financial loss or reputational damage.

Some of these are somewhat mundane but their impact should not be underestimated:

- **Loss of key personnel** can be highly disruptive where the business has become over-reliant on a handful of key individuals and these people (or teams) are poached by competitors.
- **Short-term absenteeism** is a fact of life in most treasuries. As long as the company has made a reasonable effort at multi-skilling and cross-training its workforce it is usually not too difficult to manage this risk.
- **Longer-term absenteeism,** whether planned for or not, can be more difficult to deal with – particularly where key personnel are concerned. With key personnel absent for prolonged periods, the level of operational risk within the business tends to increase.

Workplace environment

Regardless of the size of a corporate treasury team, it is often challenging to keep all members of the team 100% motivated and focused all of the time. The workplace is a complex environment. The actions of egotistical bosses can result in a poor working environment, with undesirable workplace behaviours such as favouritism and bullying. These in turn can give rise to jealousies, rivalries and disputes, all of which can cause employees to do things which may damage the company.

Let's consider what can happen when an employee feels so wronged by an employer or a boss that he decides to seek revenge…

The disgruntled employee

It is not at all unusual for an employee who, for example, has been passed over for promotion or who has had a poor bonus, to feel some anger or a sense of frustration. Even more dangerous is the employee who thinks, or knows, that redundancy is looming.

For the most part, employees who are experiencing extremely negative feelings towards the company or other employees will drown their sorrows in a bar, however, some may be motivated to seek revenge on their company, or their boss, and will want to inflict maximum damage as they depart.

Treasurers always need to be vigilant, looking out for the disgruntled employee who has the capacity to inflict serious damage on the company in an act of revenge – the IT Support person who could cause a systems crash, perhaps, or the corporate finance executive in possession of sensitive information which could wreck a deal.

Sexual harassment

The high octane environment in a corporate treasury, with well-educated, ambitious people working long hours in close proximity, can be fertile ground for cases of sexual harassment. It sometimes seems that hardly a month goes by without such a case in the corporate world. These have the capacity to be both high profile and damaging to the employer. Unfortunately they are also very difficult either to predict or to prevent.

In recent years there has been a marked trend towards lower tolerance of 'inappropriate relationships' involving corporate bosses. Higher standards of behaviour are expected of employees, particularly senior ones. Mark Hurd, the CEO of Hewlett-Packard was recently ousted from his job over such a case. This caused HP's stock market valuation to plummet – the company lost $13 billion at one point – a clear indication that the stakes can sometimes be very high.

Can employee risk be eliminated?

The short answer, unfortunately, is no, but some aspects of employee risk can be effectively managed and contained. For example:

- Provision by companies of an internal 'whistleblowing' facility so that employees are able to report any suspicious activity anonymously and without fear of reprisal has been shown to be particularly useful in combating employee fraud.
- Many treasuries employ technology which can analyse and sense-test trades input by humans and highlight them for further checking.
- Employee absenteeism levels can be reduced by ensuring that there is a positive atmosphere in the workplace.

Fortunately for treasurers in well-managed companies, there are usually robust procedures in place to mitigate most elements of employee risk and prevent problems from escalating into a company-wide crisis.

Treasurers should be able to place considerable reliance on their in-house corporate security and IT security functions.

Monitoring employee activity

In the UK over 60% of personal on-line shopping is conducted at work.

Employees on average spend at least an hour every workday on their computers doing things other than working. In many companies this theft of company time by employees is a kind of tacitly accepted low-level fraud.

Employers have tools available to them, such as network sniffer technology, to monitor this type of activity and also more serious types of abuse of the internet by employees, such as downloading offensive material and distributing it via email.

With this technology deployed in-house, fraud analysts can search, retrieve and replay every screen viewed and every keystroke made by an employee. This makes it possible to see exactly what an employee was doing over a specific period.

Other types of employee monitoring may include:

- Use of CCTV in the workplace
- Vehicle movement monitoring
- Telephone monitoring.

Where monitoring is in place, employers in most markets are under obligation both to advise their employees and to obtain their consent – this may be done through employee acceptance of a workplace Code of Conduct.

Typically an Acceptable Use Policy would be set out by the company governing employee use of business communications tools. UK employers, for example, have to comply fully with the requirements of the Data Protection Act, the Human Rights Act and the Freedom of Information Act.

Many countries have similar legislation in place. A treasurer can expect the company's HR function to be fully conversant with all applicable legislation and to ensure company-wide compliance with this.

The buck stops with the treasurer

There are many ways in which the actions of employees can threaten a company's operations.

Fortunately most threats to the company are usually extinguished before they materialise, but when they do the effects can sometimes be very damaging.

Employee risk comes in so many different guises that it can be very hard to guard against. It is, though, part of the job description of every responsible treasurer to ensure that this risk is managed as effectively as possible. ■