Businesses behaving badly

Mia Campbell suggests that accountants have a critical role to play in protecting their clients from fraudulent activity.

TEN SECOND SUMMARY

1. **Concerns over executive pay, tax avoidance, treatment of staff, corruption and lack of honesty and transparency have resulted in declining trust in business.**
2. **There has been a shift towards fraud by more senior and experienced staff and a rise in the so-called "silver fraudster".**
3. **A workforce that is supported, informed and appreciated is a key defence and can go a long way towards reducing the risk of fraud in an organisation.**

We are living in a climate of growing distrust in which high-profile corporate scandals and data breaches are eroding our trust in business while fraud and cybercrime are simultaneously eroding our trust in one another.

According to the latest Edelman Trust Barometer, trust in business has declined over the past year. Only 43% of people in the UK (falling to 38% of young people) now trust business because of concerns over executive pay, tax avoidance, treatment of staff, corruption and the lack of honesty and transparency.

These themes are commonly picked up by the media. The Institute of Business Ethics found that many of the 500 or so ethics-related stories that appeared the media last year were also about corporate culture and behaviour, the treatment of staff, and fraud and theft.

However, these issues are not mutually exclusive, they often co-exist and are inter-connected. It stands to reason that good corporate culture and leadership set the ethical tone of our businesses, our people, and our times.

The threat from within

About half of UK organisations have experienced economic crime; commonly matters such as asset misappropriation (say, stealing cash), cybercrime, procurement fraud, human resources fraud and accounting fraud. A significant proportion of these are inside jobs, committed by someone who knows the business – its people, policies, procedures and processes – well. Many more involve collusion. Although estimates vary, it is thought that at least one-third of business frauds are of this type, and that a typical organisation loses about 5% of its annual turnover to it.

But who commits internal fraud and why? The recent report by the Fraud Advisory Panel, *Businesses Behaving Badly*, found that the profile of the typical fraudster is someone with the power, access and status to recruit, commit and conceal with ease – if they put their minds to it. According to PwC, there has recently been a shift towards more senior and experienced staff and a rise in the so-called "silver fraudster" (those aged 40 and above) leading them to suggest that older people may be more willing to break the rules.

FURTHER INFORMATION

The Fraud Advisory Panel is the leading voice of the counter fraud community. It champions best practice in fighting financial crime to improve resilience across society and around the world.
Visit their website for free practical helpsheets and other resources: www.fraudadvisorypanel.org
Edelman Trust Barometer: tinyurl.com/yap6z7nu
Fraud Advisory Panel report *Businesses Behaving Badly: fraud, corporate culture and ethics*: tinyurl.com/y9fr6qt7
Higher Education Degree Datacheck: https://hedd.ac.uk/
Action Fraud: www.actionfraud.org.uk and www.actionfraud.police.uk. Take Five: https://takefive-stopfraud.org.uk/advice/
The National Cyber Security Centre: www.ncsc.gov.uk

Why people matter

People commit fraud – not companies and not (at least for the moment) machines. This means that to fully understand the insider threat we must also consider the human dimension. According to the fraud triangle, three essential ingredients are needed: the opportunity to commit fraud, the incentive to do so, and the ability to justify it.

But not everyone is a career fraudster, so what makes a seemingly ordinary employee commit fraud? Personal gain, greed, financial or family problems are commonly cited factors. But it can also be as a result of a person's experiences within the workplace. Feelings of disenchantment, a sense of injustice, or a perception of being treated unfairly can all play a part. As we have found, so can too much stress, the wrong incentives (money can sometimes change the way we think and act) and everyday tolerance of small wrongs. And this is where culture comes in.

Treating staff well and offering support to those with financial or other problems can sometimes be a very good way to prevent fraud.

The question of culture

Creating a workforce that is well-supported, well-informed and well-appreciated is a key defence and can go a long way towards reducing the risk of fraud emanating from both within and without. Organisations that do well here often have an ethical culture based on shared values and a common purpose, which is set by the board or their management team who lead by example. This makes it easy for everyone to do the right thing. Building a fraud-resilient business is a job for everyone at every level.

Internal controls

Although culture obviously plays an important part, it can only go so far. Other controls are also needed. Many executive-level fraudsters cite weak internal controls as a significant factor in their criminal decision making. Yet the Association of Certified Fraud Examiners (ACFE) has found that strong controls are something that many small businesses lack. Fewer than 16% of small businesses in their latest survey undertook fraud risk assessments and less than half had a code of conduct setting out the behaviour expected of staff. Such controls do not need to be complicated or expensive to do their job, but they do need to be well designed, consistently applied and followed, and routinely monitored and reviewed.

Although strong controls will not thwart every fraudster every time, they can certainly go a long way towards improving overall resilience. See ***Protecting the front door***.

Raising concerns with confidence

Many internal frauds are uncovered when concerns are raised by staff. In fact, about 40% of insider frauds are discovered in this way. Employees should feel comfortable asking questions and raising concerns and there should be a simple, well-publicised and hassle-free way for them to do so.

Employees also need to be able to recognise the tell-tale signs of fraud and know the types of behaviour to guard against. This is where staff understanding of policies, controls and procedures becomes important and education and training step in. Training is a useful way to improve overall awareness, gather staff views, share experiences and identify weaknesses. It will also help staff to understand that the mechanisms put in place to tackle fraud are also there to encourage, support and protect them too.

The outside threat

Although this article has been primarily concerned about the insider threat it is important to recognise that much fraud is committed by people outside of an organisation and much of this is cyber related. At least half of small businesses have experienced a cyber-attack and examples commonly include phishing emails, ransomware, and viruses, spyware and malware.

Trusted advisers

The Department for Business, Energy and Industrial Strategy (BEIS) has found that when small businesses seek external information and advice they are more likely to turn to their accountant than almost anyone else. It follows that small businesses, which are concerned about fraud or fear that they might have become a victim, are also likely to go to their accountant as their first port of call.

As a trusted adviser, an accountant's knowledge is their commodity and this needs to be kept up to date. So said IPA CEO Andrew Conway in the November/December edition of this magazine, but this can sometimes be a challenge in the rapidly changing area of fraud and cybercrime. Thankfully, help is at hand through a growing body of free guidance and fraud alerts emanating from initiatives such as: the national fraud reporting service run by Action Fraud; the national awareness campaign, Take Five; and the National Cyber Security Centre.

Accountants therefore have a pivotal role to play in protecting not only their own businesses but those of their clients from fraudulent activity.

PROTECTING THE FRONT DOOR

Career fraudsters sometimes deliberately seek out positions in organisations that are perceived (or known) to have weak controls and an over-reliance on trust. This can leave small businesses particularly vulnerable to the threat from within.

Basic screening of candidates should include the following.

- Ask to see original identity documents (if there is uncertainty on whether they are genuine use a document verification service).
- Check qualifications either directly through the issuing body or the Higher Education Degree Datacheck service.
- Take up work references, call referees and probe any employment gaps.

Mia Campbell is the Manager of the Fraud Advisory Panel. She has been involved in the counter-fraud field for more than 14 years and regularly comments on financial crime matters, particularly those affecting charities and small businesses.
T: 020 7920 8721
E: Mia.campbell@fraudadvisorypanel.org