

SCREENING AND VETTING

WHEN TO SCREEN? WHEN TO VET?

Are you doing enough to prevent criminal activity within your company?

Prevent fraud, violence and/or terrorist activities in the workplace through the use of employee screening and vetting.

Terrorist attacks, security breaches, theft, fraud, violence and drug and alcohol abuse are on the increase in the workplace so you've got to ask the question – are we doing enough to prevent criminal activity within our company?

Criminal activity in your business is more likely to be committed by your employees than from someone walking in off the street.

It is your responsibility to ensure that you are not putting your people, your assets and your company at risk and, thereby enabling individuals to slip through the net so that they may go on cause damage elsewhere.

An effective way to prevent fraud, violence and terrorist activities in the workplace is through the use of employee screening and vetting.

This article looks at how you can identify people who represent a risk to your business, prior to or during employment by you, using employee screening and vetting.

USEFUL WEBSITES

www.bbc.co.uk BBC NEWS
www.bsi-global.com
www.banksafeonline.org.uk
www.cifas.org.uk

Vetting and security screening are the first line of defence in preventing infiltration and identifying staff susceptible to collusion or opportunistic frauds.

Source: CIPD/CIFAS Joint Report 2007

ARE WE DOING ENOUGH?

To answer this we need to look at the level of fraud, violence, criminal damage and risk through drug and alcohol abuse occurring each day in the workplace.

It is difficult to establish the scale of employment fraud and to estimate the cost to the UK economy because it has rarely been measured and many businesses are reluctant to admit losses. However, a recent report by CIFAS - the UK's Fraud Prevention Service has confirmed that staff fraud is now emerging as the single most significant fraud risk to the financial services industry and a serious risk to all businesses. British retailers are winning the battle against shoplifters but the UK is one of the worst countries in Europe for stealing by employees, costing employers £billions. The UK was second behind Iceland in a study of employee theft in nations, according to a 2005 Retail Research Report.

Insider fraud is also currently the number one threat within the financial services sector.

Case Study:

In June 2006, Donald Mackenzie was jailed for ten years at the High Court in Edinburgh for embezzling £21 million from the Royal Bank of Scotland (RBS).

He was caught after the RBS introduced a new loan-guard computer system. He accessed the money through the bank's loan system by setting up false accounts in the names of fictitious customers at a branch in Edinburgh. Mackenzie had been named Manager of the Year for three consecutive years from 2002.

In a survey conducted by Halifax Bank of Scotland (HBOS) plc it was found that 24 per cent of Small to Medium Size Enterprise (SME's) in the UK have suffered from staff fraud, however only two per cent identified it as being a frequent problem. Nineteen per cent of companies with fewer than 15 employees have experienced staff fraud; this is significantly higher at 48 per cent with companies that have 36 employees or more.



WHAT IS FRAUD

The Fraud Act, which became law in January 2007, broadly defines three main types of fraud:

Fraud by false representation where an individual dishonestly makes a representation that is untrue or misleading eg impersonating someone in order to gain access to their financial accounts.

In a world of constantly changing threats, background screening is a first line of defence. Successfully implemented screening reduces the risk to a company from potentially fraudulent employees.

Many companies have some sort of security measures in place to monitor the activities of its staff, customers and even intruders in an attempt to deter theft and fraud. CCTV captures and records the fraudulent event as it occurs and security guards can respond to the breach after it has happened but vetting and screening is a preventive measure to exclude rogue people from being able to commit fraudulent acts while under your employment. Screening and vetting can also help companies identify personnel who might be prone to violence, alcohol or drug abuse, or who might have connections to unlawful organisations.



SCREENING

A 2005 Mori poll found that 30% of applicants admit to lying on their CV, and that 34% of managers don't check the background of most applicants because it's too time-consuming. In some organisations, the 'know your customer' checks carried out to comply with Financial Services Authority requirements for opening new customer accounts are sometimes more rigorous than those in place for employing new staff. Yet screening applicants is vital in order to:

- Verify identity
- Confirm previous performance
- Ascertain integrity

Source: Control Risks Screening.

All applicants for employment should complete generic corporate application form rather than simply submitting a CV. The information employers should consider specifically requesting on their application form includes:

- A full account of any gaps in employment.
- The candidate's reason for leaving their previous employment. Confirmation, if relevant, of the candidate's permission to work in the UK.
- Any involvement in external businesses and details of directorships held.
- Details of any civil criminal proceedings that may be pending.
- Details of any convictions that are not considered spent under the Rehabilitation of Offenders Act 1974.
- Details of any bankruptcies or county court judgments or defaults.
- The number of days' absence due to injury or illness in the most recent 12 months in employment.
- Full details of candidate's qualifications and employment history.

The form should be signed, should include a declaration that all details are correct and include notification of candidate consent to any background checks being carried out.

Candidate details should then be verified, using documents such as passports, driving licences, EEA member state ID cards, utility bills (NOT mobile phone), bank or mortgage statements, benefit books, rent cards and income tax statements.

Written references and educational qualifications should also be verified. Electoral rolls can be used to confirm addresses.

SCREENING CHECK LIST

- Credible working history check
- Initial check is a minimum of five years
- Once 16-week probationary period completed, the work history check can be extended to 10 years back
- Checking of security personnel is governed by BS7858
- The person/organisation performing checks on security personnel must comply with BS 7499
- Reference check from previous employers
- Personal character reference from individual that has known the candidate/employee for at least five years
- Proof of identity, current address and residency
- Psychometrics

VETTING CHECK LIST

- Criminal Records Bureau (CRB) can provide records as far back as 14 years of age
- For certain roles within different industries checks are performed on a regular basis
- For security operatives a criminal records check is used as a one-off in line with the Security Industry Authority (SIA) regulations. It is a maximum of five years criminal history
- For crimes like murder, it is struck off records after 10 years
- UK citizenship
- UK residency in the UK for the past five years

25 years of expertise providing total security solutions



Fraud by wrongfully failing to disclose information eg on a CV.

Fraud by abuse of position where an individual in a position of trust over another person's financial interests dishonestly and secretly abuses that position.

REPORTING FRAUD

KPMG have found that attitudes towards reporting colleagues had changed with employees more inclined to report fellow members of staff for fraud. In the UK, 83 per cent of workers questioned said they would report colleagues involved in major fraud.

In Scotland 1,800 people participated and it was found that 77% of those questioned would report colleagues involved with major fraud. Moreover, 43% said they would report minor fraudulent incidents to management.

What is scary is that in a survey conducted by Leicester University, a staggering 70% of the 2,000 people questioned said they would commit fraud if they knew they could get away with it. In the light of this it's not surprising to find that fraud in the workplace is on the increase.

DRUG AND ALCOHOL ABUSE

Then there is the issue of drug and alcohol abuse in the workplace. Time Out magazine found that in one in three people that they questioned had taken drugs such as ecstasy, cocaine, cannabis and amyl nitrate at their place of work.

On average 15 million working days per annum are lost as a result of alcohol and drug use in this country.

Source: www.hrmguid.co.uk E-news 08 January 2004.



Where the job role involves the personal safety and security of the general public, organisations do drug test their employees. Railtrack randomly test five per cent of its employees; BP tests all employees who work offshore, and Shell UK routinely test key personnel.

Does your company conduct regular drug testing of employees?

VIOLENCE AT WORK

Violence at work is also affecting the operation of staff and companies. In 2007/08 almost a million people were attacked at work. Security, nursing, social care and public transport workers are more likely to be attacked than in any other sector.

More than three million working days are lost every year due to violent incidents at work. The cost to the industry in compensation and lost production is hundreds of millions of pounds. Half of reported physical attacks and a third of verbal threats come from people known to the victim.

THE RISE OF ORGANISED CRIME

Over recent years we have witnessed an increase in workplace security breaches, sometimes as part of organised crime. We have also suffered devastating terrorist attacks through an organised global network.

Criminals have been able to gain jobs throughout various market sectors and defraud companies out of millions of pounds a year and in the worst cases destroy property and kill innocent people. Prevention depends as much on internal vigilance as on having appropriate procedures in place to either weed out or block the criminal element from your business.



GETTING IT WRONG

The Financial Services Authority (FSA) has investigated security measures and systems at 18 UK high street banks, insurers, financial management companies and stockbrokers. It has revealed that criminals involved in organised crime are applying for jobs in financial institutions so they can commit fraud. The report highlighted that identity fraud was the main breach with criminals using private information to gain money, goods and services.

Virgin Home Energy had to dismiss two recruitment agencies they were using to hire staff after they supplied rogue employees. An internal investigation revealed that between 12 to 14 people were fraudulently signing up customers in London. It was possible that the sales staff filled out the forms by obtaining information from the electoral register from public libraries. Criminals can also obtain private and confidential information from mobile phones, personal organisers and social networking sites, such as Facebook.

So what can companies do to keep criminals out of their business?

VETTING

In 2006, The Royal Mail was handed a record fine of £11.4m for failing to effectively prevent mail being lost, stolen or damaged. During investigations Postcomm, the regulator directly identified poor vetting of staff as the primary cause of the problem.

Vetting candidates/employees takes screening a step further by performing criminal records checks. The Criminal Records Bureau (CRB) can provide records as far back as 14 years of age. For certain roles within different industries checks are performed on a regular basis. For security operatives a criminal records check is used as a one-off in line with the Security Industry Authority (SIA) regulations. A maximum of five years criminal history is released to the employer. Given that the motivation for the majority of staff fraud is financial gain, a Credit Reference Agency (CRA) check is crucial when vetting staff who will have access to cash.

USING YOUR SCREENING AND VETTING POLICY AS A POSITIVE MARKETING TOOL

Increasingly when submitting tenders for large contracts, companies are expected to submit various company documents - including: Environmental Policy, Health & Safety Policy etc. By creating a corporate screening and vetting policy that clearly demonstrates your company has a responsible and secure method for recruiting staff with impeccable credentials, you can improve your credibility with prospective customers. Voluntarily submitting this with any contract bid will enhance your reputation for corporate responsibility.

USEFUL REFERENCES

- * British Standard (BS) 7499:2007 Static site guarding and mobile patrol services
- * British Standard (BS) 7858:2006 Security Screening of individuals employed in a security environment. Code of practice.

CIFAS is a fraud prevention service, covering the United Kingdom. It was created in 1988 by a group of retail credit companies. All the organisations that participate in CIFAS are committed to sharing information and expertise to develop best practice in the fraud prevention field. Members are also committed to tackling fraud-related crime in the public interest and to developing closer relationships with the law enforcement agencies.

WHEN TO SCREEN AND WHEN TO VET?

The screening process is used to validate the employee's character, skills, and their suitability for the role.

However, when a candidate/employee is being considered for a position that demands responsibility and trust and where there is a statutory safety requirement vetting will almost certainly be required. See examples below:

Job	Location	Screening	Vetting	Supplementary Vetting
Cleaner	Cleans office car park	YES - character and work references	Not Required	Not Required
Cleaner	Cleans cash office	YES - character and work references	Criminal Records check - CRA	Not Required
Cleaner	Cleans School	YES - character and work references	Criminal Records check	Criminal Records check Bureau
Porter	Apartment Block	YES - character and work references		
Porter	Bank	YES - character and work references	Criminal Records check - CRA	
Porter	Hospital	YES - character and work references	Criminal Records check	Criminal Records check Bureau

If possible, it's good practice to vet temporary and agency staff to the same level as permanent staff.

Increasingly, organisations now outsource all or some of their screening and vetting to outside agencies. Although there is no single independent body you can turn to for vetting and screening advice, we do recommend that you use a practitioner compliant to BS 7858. Agencies with experience in risk management particularly business security risk management also have good track records in security screening.

Some trade bodies have their own self screening process as part of the membership criteria. A good example is the FSA which performs a security screen on each new member application.

Case Study: Capita Group plc

A subsidiary of the giant Capita Group became the first firm fined by the FSA for having poor anti-fraud controls after some of its staff helped to defraud customers. The FSA fined Capita Financial Administrators (CFA) £300,000 when their findings were published in March 2006. The FSA said that 'CFA did not take adequate steps to ensure that it had effective controls to reduce the risk of fraud. There was a specific failure in training to raise awareness of fraud risk and HR procedures to verify that adequate references had been received. This resulted in a material risk that new staff were not competent or lacked integrity.

Security screening and vetting is important for the defence of your business from rogue employee's intent on damaging your ability to trade. Understanding the difference between screening and vetting, the context in which they apply and where you can go to for help will put you in a better position to protect your business.