



Screen test

A recent survey of staff recruitment agencies revealed a worrying lack of compliance, understanding of legal requirements and adequate screening of agency staff. **Michael Stephens** and **Norman Mortell** outline the findings and provide some recommendations.

The background

The recession has led to an increase in the use of temporary and agency personnel, with many organisations utilising a core of permanently employed staff supplemented by agency and contract staff, with recruitment agencies being used as an extension of the Human Resource function to source and select new contract and full-time staff.

But how well do their checks work? According to information obtained by the *Mail on Sunday* in January, some 349 illegal immigrants – sourced via recruitment agencies – were working within Whitehall departments, Councils and NHS Trusts. Not properly vetting staff may leave

an organisation vulnerable to fraud. For example, an accountant at a Birmingham-based property management company took more than £350,000 from his employers by transferring money from clients into accounts in his own name, despite already having a history of committing theft and deception under a different name. Not surprisingly, there is growing concern amongst larger organisations that while they themselves are carrying out thorough pre-employment checks on their own staff, the same level of rigour may not necessarily be built into the pre-employment screening processes of third party suppliers.

Serious concerns in Government over illegal workers, terrorism and data ►

and information loss led to the Government making public the Security Policy Framework in 2009. Built into the framework is the requirement to be vigilant during the recruitment process, with specific reference made to the Government's Baseline Personnel Security Standard (BPSS). Other guidelines such as those issued by the Centre for the Protection of the National Infrastructure (CPNI) have been developed to assist organisations in

reviewing and developing more robust procedures. ISO27001: Information Management Security Standard is another example of how self-auditing and review against standards can greatly improve the security of an organisation's valuable data and information.

The test

A major medical research organisation, the Medical Research Council, took the decision to conduct a security

audit of its staff agencies. During the second half of 2009, 35 recruitment agencies, providing a wide range of interim, temporary and permanent staff, were audited. The candidates ranged from senior management to junior administration staff; some were permanent staff appointments and some were temporary; some were supplied from niche markets and some worked within a small geographical area. All were inspected for

both their compliance and understanding of the BPSS and general security processes. Agencies were informed in advance of the review and asked to identify an employee with the necessary authority to participate in the audit. The responsible employee (usually a manager, executive or audit specialist) was then contacted by the reviewer and appointments were made. The two key areas were the understanding of BPSS and general security.

DETAILED FINDINGS

Key controls

Most organisations had a least a rudimentary process in place, with owners or senior employees entrusted with the keys to the offices. But 9% had no key control process in place.

Hard copy information security

Because of the sensitivity of information being held on employees and candidates for clients there was a high degree of compliance with the recommendation to hold such potentially sensitive data in secure cabinets. Some offices had secure cupboards or small rooms which provided the same level of security. While there is a healthy 83% compliance, there is still a concern that sensitive documents may not be locked away by 17% of those audited.

Clean desk policy

Although 83% of those audited had provision to store sensitive data in secure cabinets, it is concerning that 37% do not have a clear desk policy. This infers that information may be being left on desks and not placed into secure cabinets.

Data destruction policy

Having a data retention and destruction procedure is part of the requirements of the Data Protection Regulations. The secure destruction of confidential and personal information is therefore an essential issue for agencies. The feedback that 49% of those audited do not have a data destruction policy is of concern. This is a serious issue and should be included in a data protection policy to ensure that the organisation is in full compliance.

Secure email / encryption

83% had no process for secure email or encryption. This may be because the use of such processes is not mainstream yet. Organisations should review what information is being sent out via email and consider whether some level of security should be put in place to protect business sensitive and/or personal information.

Access to BPSS

One of the primary reasons why the audit was conducted was to assess the level of knowledge and compliance in relation to the BPSS. 43% had either a good knowledge or a reference copy but 57% did not have access to the BPSS and so would find it extremely difficult to comply with its requirements.

Screening policy

The majority of organisations had a screening policy in place but 26% did not, and that is of concern. The screening process needs

to be documented so that staff can ensure that all aspects are covered in the screening to meet the clients' needs.

Referee positively identified

60% of the audited organisations took some steps to ensure that the referees provided were bona fide. However, some of these did little more than accept a company email address for the referee. A worrying 40% never checked the authenticity of the referee.

Open source checks

Given the availability of information, and free search tools on the internet, it was surprising to see that only 29% of those audited used open source checks as part of their screening process. Those using open source checks used mainly Google searches and Linked In for executive appointments.

Domestic extremism checks

The UK Government is concerned about terrorism and about extremists infiltrating organisations. Some groups, such as animal rights activists, have been particularly active in this regard. It is a serious concern that 74% of the organisations did not carry out a domestic extremist check and an additional 12% simply asked the candidate at interview. Only 14% actively carried out this check by using third party suppliers. Given the nature of the client's business this seems to indicate a lack of knowledge of the client's needs.

Right to work checks

Although 63% check a variety of documents, and 29% check the Visa alone, the check in some cases is cursory. Many reported that they just carry out a visual check or copy the documents rather than checking at source that the documents are genuine. Others get the individuals to sign to say that they are genuine. 3% said the responsibility lies with the client, which is true, but if the client is expecting the agency to conduct this check then it could become a grey area with neither party doing it. One agency stated that they only recruited UK citizens and so didn't do any checks. However, what if the person was not really a UK citizen and was using an assumed identity and/or fake or stolen documents?

ISO9001 Certification

There was a direct correlation between the 26% of organisations with ISO9001 certification and higher levels of compliance. ISO9001 is only one of a number of quality management processes and 74% seems a high percentage of suppliers not to have a quality process.



“In January 2010, some 349 illegal immigrants – sourced via recruitment agencies – were found to be working within Whitehall departments, Councils and NHS Trusts.”

The BPSS describes the pre-employment controls for all civil servants, members of the Armed Forces, temporary staff and government contractors. The mandatory pre-employment controls required by the BPSS have been adopted to address the problems of identity fraud, illegal working and deception. Failure to adopt the BPSS requirements could pose a serious risk to reputation, integrity and financial assets. As a minimum requirement, all staff mentioned above must be subject to the BPSS.

The BPSS comprises verification of the following four main elements, which are described as the RICE requirement:

- Right to work, nationality and immigration status (including an entitlement to undertake the work in question).
- Identity confirmation.
- Criminal record (unspent convictions only).
- Employment history (past three years).

Questions were also asked to determine if the company had undertaken the ISO9001 quality process or adopted information systems security protocols, to protect data, utilising software or other standards such as the CPNI, ISO 27001 or the (US) Sarbanes-Oxley Act 2002. In total, nearly 50 control items were tested at each agency.

The findings

Most agencies recognised the need for security of data (either written or electronic) but few had received expert advice on basic security procedures and, consequently, significant flaws were found in their security arrangements. Agencies that specialised in recruiting senior interim staff appeared to have fewer controls, but this was not necessarily a flaw because they recruited at senior executive level and their candidates were generally well known within the industry.

Generally, the recruitment agencies were unaware of the BPSS requirements, though

where a company had an internal audit department, or quality process, there appeared to be a more thorough understanding of the requirements. Large companies had the resources to provide their employees with online tools such as an intranet, and this proved positive in facilitating further education and acting as a reference guide. Small or specialised agencies had a more intimate knowledge of their candidates and were able to introduce new policies and procedures very quickly. All of the agencies were prepared to review processes and enter into contractual requirements to implement the requirements of the client.

The recommendations

Few agencies had any knowledge of the BPSS but all insisted they would follow the BPSS if required to do so. It was therefore recommended that the requirements of the BPSS were included in tender requirements, Service Level Agreements and contracts, including provision of the clients

to audit the process and for the agency to provide evidence that the processes are working to the required standards.

For those companies involved in the supply of interim senior managers it was recommended that they meet with the client to discuss security issues and concerns, and to familiarise themselves with specific issues such as domestic extremism, particularly in relation to secondary targeting by these groups, which may affect them directly. Following the review of the other security elements that were tested, it was recommended that a complete analysis was undertaken in determining the overall suitability of agencies prior to conducting work with them.

Advice

Firstly, if you use an agency, ensure that they understand your requirements with regards to pre-employment screening and security of information and systems. Stipulate the security requirements in contracts and require that evidence is provided to reassure you that they have fully complied.

Secondly, if you are a supplier or agency, it is vital that you take steps to protect your organisation by referring to security guidelines such as those from the CPNI, to ensure that you have taken steps to assure your clients of your compliance with the various legal and regulatory requirements, and that robust and comprehensive processes are put in place when screening candidates.

FURTHER INFORMATION

Agenda Security Services:
www.agenda-security.co.uk

Medical Research Council:
www.mrc.ac.uk