www.counter-fraud.com

New Website

Fraud Intelligence

For the prevention, detection and control of fraud in all its guises

Watch your back

Government bodies and companies, typically, no more expect to find enemy infiltrators among their ranks than the revelling Trojans anticipated the crafty Greeks. But, as ***Peter Tickner*** *knows from experience, fraudsters may slip in surprisingly, uncomfortably close.*

"Yes, I know that address, that's *****'s house. He's a successful armed robber, very successful. It's a large detached house with electric gates, swimming pool and guard dogs. I wouldn't go anywhere near him if I were you." These were the words of a police collator to my internal audit team. We'd been trying to track down a maintenance contractor who, as it turned out, was a Trojan at Scotland Yard.

Trojan fraudsters come in broadly two types, each equally potentially lethal to your organisation. There is the employee Trojan – and often these will infiltrate at a surprisingly low level in the hierarchy. Then there is the contractor or organised Trojan where either a company or a number of deliberately placed employees will conspire to use your organisation to commit serious fraud or destroy the organisation by fraudulent and corrupt means.

The need for effective vetting

The key to trying to prevent a Trojan fraudster from infiltrating your organisation is to have an effective means of vetting applicants as staff or contractors. Unfortunately, many organisations simply do not have an effective system at the point of recruitment. Most UK government departments and agencies rely heavily on a vetting system designed primarily to protect national security. Local authorities do not generally have any standard checks when recruiting new employees or contractors, although most will apply similar checks to the information supplied in the application form or submitted CV. Larger commercial organisations can have some sophisticated checking of applications and those working on certain types of government contract will use the government's national vetting system as well.

The only common checks that most organisations apply at the recruitment stage are to check references from a previous employer. Many ask for an employment history but I cannot think of any HR departments that, once they have a potentially successful candidate, then check out the validity of their employment history since the individual left the education system.

Any apparent gap in the employment record should be a cause for concern, starting with working out when the candidate left school or university and comparing that information with stated institutions and their claimed age at that time.

Trojan employee – example 1

An example of how ineffective this type of checking can be arose during one of my earliest cases at Scotland Yard, in the late 1990s: a fraudster was found entirely by chance when two police officers arrested another individual. Documents in the back of the arrested individual's vehicle showed contact with a police employee working in the HR department on the 'back record conversion team'. When the police subsequently arrested the Metropolitan Police Service employee, they found a briefcase in his possession containing information stolen at work for use in fraudulent activity.

The back record conversion team was at the time taking manual HR records about individual employees, weeding out any information no longer needed and then preparing the files for input into a new electronic HR system. This was a very dangerous part of the organisation in which to find a fraudster. So how had he evaded our recruitment checks in the first place?

The Trojan in question was skilled at getting work in government organisations; when the police investigated we realised that we were at least the third government body to have employed him.

One of the golden rules of this type of fraudster is that they are not overly ambitious. They don't set out to get an important position; they'd much rather have an administrative or supporting role. First, the standards needed to get the job are usually lower and the quality

of other candidates less strong, thereby increasing the chances that they will be successful in getting the appointment. Second, they attract less attention in support and backroom jobs, giving them more time to carry out their nefarious activities. Third, they usually are successfully gambling that less rigorous checks will be applied to the filling of less important posts.

Our back record conversion Trojan had been very careful about how he had engineered his own 'back records' when making his original application for the first administrative job that he had secured in the MPS, as a clerk involved in payroll preparation. His first government post had been with the Charities Commission, who, indeed, seemed to have lived up to their name by employing him. He provided references of a previous commercial employer, 'Johnson and Company', whose 'personnel office' subsequently provided a written reference in glowing terms.

The passport he provided as proof of identity contained an interesting clue. It gave his height in metres and centimetres. On his application and in person his height in feet and inches was nearly a foot taller than the metric measurement on the passport that he produced, supposedly with his picture as an adult only a year before. However, no one noticed the considerable height discrepancy.

While our Trojan fraudster worked at the Charities Commission he was well regarded and whatever he did there that he shouldn't, never came to light.

He resigned from the Charities Commission after he applied for and obtained an administrative post in the Ministry of Defence. For this job, he managed to produce a UK resident's passport with his right height. The MoD applied some stringent checks through their national vetting process for the post that he then took up. He gave two references, the Charities Commission and 'Johnson and Company'. This time 'Johnson and Company' changed address but the reference returned with the same company stamp seen by the Charities Commission.

Whatever he was up to at the MoD never came to light, but after a period of unexplained absence when they discovered that the telephone contact number he had given them didn't work and they couldn't find anyone at the address that he had given them, they sacked him in absentia.

He appeared to have no gainful employment from the time the MoD noticed that he had gone missing to the time nearly a year later when he applied for an administrative job with the HR department of the Met.

Of course, he now had a problem, as plainly he could not put down on his application form that his last employer had been the MoD, or any check would have revealed that they had sacked him. So, creatively, he solved the problem by putting down his home address at the time as his last employer's address, and put the contact details for the office as his then home telephone number. I am sure that you will have anticipated the name of the company by now – it was of course 'Johnson and Company' – at what, as well as being his home address, was also the address given to the MoD as his previous employer's location. He now no longer showed them as his employer before the Charities Commission but instead showed that he was previously unemployed or a student. When the local Met HR manager checked out the employment with 'Johnson and Company' by ringing this 'office', his wife obligingly answered the phone and gave a glowing reference for him. Later on, a duly completed written reference in similarly glowing terms turned up from 'Johnson and Company' with the obligatory company stamp used on the two earlier references.

There was a further twist of irony, not lost on us when all this came to light later. His wife was at the time employed as a temporary local clerical assistant at the local police station! As she was only employed as temporary clerical cover, no one had applied any checks other than putting her name and address into the basic criminal records check, where nothing untoward had shown up.

Had anyone sought to verify this company with Companies House records, they would have discovered that although there was indeed a 'Johnson and Company', it had no connection with any of the addresses that had been used by the fraudster; nor were any of its directors those named on the letterheads for the references sent to his future employers. He had simply picked the most generic company name that he could think of – but even so a careful check would have revealed the fraud before anyone had employed him.

This type of Trojan fraudster is always catholic in their tastes and will turn their hand to anything of potential advantage. In the time our Trojan was with us, he cross-fired a dud cheque, stole a valuable ring, fraudulently altered police warrant badges passed out to his fellow gang members, ran a fake charity using police systems and stole a number of differing blank documents with police letterheads. He also copied the bank account and personal details of a number of staff with the intention of committing identity thefts later on.

During his time as an administrative officer with the MPS the Trojan was employed as a payroll clerk, then as a clerk in a police station and finally moved back to HR again. In each area of the business, he found new frauds and fiddles to turn to his advantage.

Tightening the noose on employee vetting

The police have long been aware of their own vulnerability to infiltration by criminal Trojan employees, not intent on financial fraud but often on stealing or altering police information about themselves and their partners in crime. In part, the access that the police have to prior criminal records and intelligence databases about suspected or known criminal contacts helps in the fight against this kind of infiltration, as does the use of undercover police officers, their own Trojans, to infiltrate the criminal gangs that try to infiltrate the police. However, such methods are not available to most organisations.

It is far better to root out fraudulent putative employees at the application stage, than to discover later on that they are fraudsters. Most will lie somewhere on their application form and that should be capable of discovery during final checks. It would be too labour-intensive to subject every application form from potential employees to a rigorous check. However, once a short-list has been drawn up of candidates it is worth considering checks of factual information supplied about previous employment history, including testing whether business referees appear to be genuine and if their phone and address details are correct. Personal referees are an almost pointless check. All it shows at best about the candidate is that they know someone prepared to act as their referee.

It is also important that when candidates turn up for selection interviews or tests they are asked to bring original documentation about themselves to be checked. If possible, passports and ID cards should be checked visually against the candidate who turns up and if there is a staged selection process then the original candidate should be photographed for comparison with the candidate who turns up for the next stage.

Checking for fraudulent recruits

Details that can be verifed include the National Insurance Number. If they were born in the UK it is possible to check if the NI number is genuine by comparing the code to their stated date of birth. The final code changes according to the time of year and the start codes can be identified to a particular year. For those born overseas with UK employment rights, their NI number should coincide with the time when they were first granted employment status.

It is not uncommon to find duplicate NI numbers and they are not always a fraud. However, if you find an unrecognised code or one that doesn't look right it is a pointer to a potential fraudster.

Do they frequently change home address or bank account details? If there are repeated examples of this I would take a keen interest in finding out why.

If it hasn't already been verified, check out the employment history for any gaps or unusual employers.

The Trojan company

They will want to be your contractor to get something tangible out of you to which they are not entitled. Sometimes they will be 'sleepers', looking to build a cosy history with your organisation before they strike; in other instances they will be trying to take advantage from day one.

Most organisations have a range of potentially 'dodgy' contractors in certain obvious areas of business, including security, minor works and maintenance, and catering. These activities, for which the basic wages of the contractor's employees or in-house staff will be relatively low, are where Trojans are most likely to strike. They will ruthlessly undercut competitors to ensure that they get the contract. And, once they are in, will set about getting their 'payback' out of your organisation.

The simplest type is the Trojan security company, which either provides security guarding or security devices, but in fact uses them to spy on your organisation or to steal assets. In similar vein, Trojan cleaners will sweep business offices, literally, looking for useful documents and papers about your business that they can turn to fraudulent usage. When I ran the audit department for Scotland Yard, I always insisted that our offices were only ever cleaned when we were present to supervise and could ensure that they didn't see any sensitive papers.

Because of the nature of the business of Scotland Yard, we had a particular problem with Trojans, especially in the areas of backroom support activities. They were invariably after internal information and wanted to know how much the detectives who dealt with organised crime knew about them as well. The police were fully aware of this, but some still managed to get under our radar.

Armed robbers who dropped in to fix the Flying Squad's offices for them

I know, it sounds so unlikely that it is hard to believe, but it actually happened. I stumbled across the company run by an armed robber by accident when a quantity surveyor mistakenly misspelt the name of

a contractor during a search for companies connected to another case.

When I pulled out the contract file for the company, I realised immediately that something was wrong. They gave an address of a business park and a mobile phone for contact. But by chance, I knew that there was no business park in that area. We telephoned the local police intelligence collator and got the astonishing reply: "Yes, I know that address, that's ★★★★★'s house. He's a successful armed robber, very successful. It's a large detached house with electric gates, swimming pool and guard dogs. I wouldn't go anywhere near him if I were you."

How on earth had an armed robber ended up with a contract from the police to provide minor works and maintenance to police stations and specialist police units?

Our finance department provided basic financial checks on new companies and at the time used a member of staff in the Works Department to do that for new contractors. He had called for the latest set of accounts lodged with Companies House and on checking had found discrepancies between them and the accounts submitted by the contractor. He drew these to the attention of a senior works manager but was overruled and a note was put on the file that "as both sets showed the company in profit" it was no bar to their award of contract. Quite extraordinary!

The second curiosity was how this firm was on the list of invited bidders in the first place. Company 'A' had recommended a small company 'B' to fill the spot when our quantity surveyors needed more bidders.

Both A and B now had my full attention. While my staff started hunting through invoices to check out the work that had supposedly been done by A and B, I pulled the contract files for A as well. A had been on the Met's list of minor works contractors for a few years, but when I looked back at their original references something struck me immediately. A was effectively a two-man company with two directors who ran and owned everything, supported by a varying army of permanent and temporary workers. One director of A had an unusual surname, so it was a bit of a giveaway when the firm that had provided their reference to get on the books in the first place turned out to include the same man!

There was also something odd about the business address of A: although it clearly was a business address this time, it still rang a bell with me. I went back and looked at B's contract file. The answer lay in their annual return submitted to Companies House. B had already used their home as their business park address; it would have been a bit awkward to show that they were also living there, so they had used A's work address as if it was their address.

At the time, we had no idea who had really turned up on some of the jobs they had done. What we did discover – and it led to urgent remedial action by the police – was that our armed robber had been responsible for carrying out routine maintenance work inside part of the Robbery Squad!

Whatever type of organisation it is, if there is something that a Trojan can gain by infiltrating it they will. On the surface, it seems incredible that a convicted armed robber's company could have so easily ended up with a contract to work for the police. But they had help from others to 'get in' and, once inside, were accepted as part of the 'background noise' supporting the police.

Peter Tickner *(info@petertickner.co.uk, 07768 033821) is the author of 'How to be a successful frauditor'. His new book, 'The successful frauditor's casebook' is due to be published by Wiley in April 2012. See www.petertickner.co.uk.*