The enemy within: the inherent security risks of temporary staff

Ching Liu

Ching Liu, Control Risks

Since the credit crunch and the subsequent tentative recovery, there has been a boom in the use of temporary staff. According to the Chartered Institute of Personnel and Development's (CIPD) Labour Market Outlook Survey last year, employers reported that 29% of new recruits will be employed on this basis.[1]

One, perhaps unexpected, result of this growth of temporary recruitment has been the emergence of a new kind of fraud: CEO or executive-level impersonation. This kind of fraud starts with a member of the fraudsters getting a temporary job within the organisation, working out its systems and culture and identifying potential 'weak links' among its staff who can be subsequently exploited.

Using this information, the fraudsters will then impersonate the company's executive to authorise payments or divert funds to spurious companies or bank accounts set up by the fraudsters. Profiling the CEO or other senior staff members in this way enables the fraudsters to circumnavigate the company's usual checks and controls by asking for payments to be made manually and/or confidentially. By this stage of the scam, the temporary employee will usually have long left the organisation and is unlikely to actually transact the fraudulent payments him- or herself.

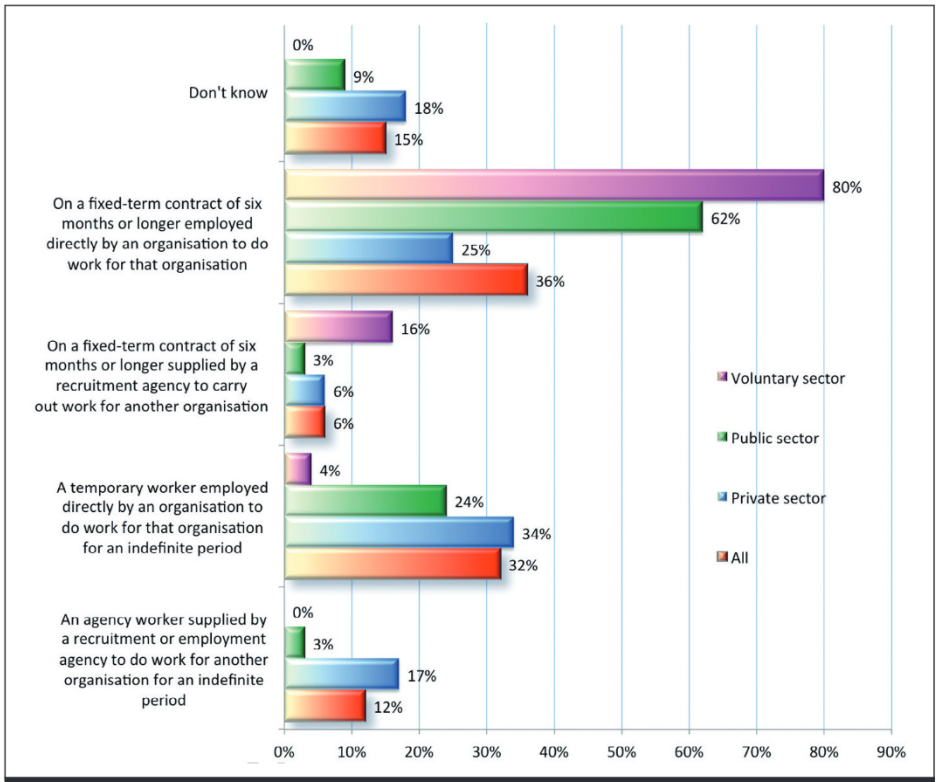
"Impersonation frauds are not dissimilar to the age-old problem of industrial espionage, but with a more direct financial gain for the perpetrators"

The understanding of the company's processes and personnel gained will be well in excess of any run of the mill attempts to submit fraudulent invoices or other common scams, and the fraud is far less likely to attract suspicion, especially if the person making the payments has been carefully selected beforehand. It does not necessarily need to be the chief executive whose identity is assumed by fraudsters – any senior member of staff with the authority to authorise payments outside of the company's normal procedures will do. Impersonation frauds are not dissimilar to the age-old problem of industrial espionage, but with a more direct financial gain for the perpetrators.

How it works

So how does it work? Typically, once the fraudster has embedded him- or herself as a temporary employee, he or she will get to work learning the firm's systems, procedures and culture as well as establishing the identities (and personalities) of key senior executives.

The more information they gather, the more credible their future attempts at



Types of contract under which temporary staff are employed. Source: CIPD Labour Market Outlook Survey.

extracting payments from the company will be. To this end, they will usually engage in social engineering – getting to know key people both inside and outside of work – to ensure that their knowledge is as comprehensive as possible. In this way, embedded fraudsters need not even work in the sensitive area if they can get useful information by socialising with those that do. This also enables them to identify who will be the (unwitting) target of their operation – usually somebody in the accounting function – when they move to phase two of the fraud.

"Often fraudsters will use third-party websites that allow spoofed emails to be composed and sent via a web front-end"

Once a profile of the company's systems and staff has been created, the fraudsters are ready to put their plan into action. This will usually involve the fraudsters making contact with the weakest link they identified earlier, initially by phone and subsequently by email, using a spoofed email address to replicate the senior person's email address. Such spoofing is easily achieved and often fraudsters will use third-party websites that allow spoofed emails to be composed and sent via a web front-end.

Over the course of the communications, the fraudster will attempt to persuade the employee to send funds or pay fake invoices outside of the company's usual controls, relying on the seniority of the purported CEO or executive level recruit to ensure compliance.

The fraudsters will often tell the weakest link that the payments are to be made 'off the books' because they relate to a confidential deal that cannot be made public. They may also include written authorisations that appear to contain the correct signatures, although these will usually have been copied or faked. The overall impression on the member of staff asked to make the payments is often highly convincing, and may also be accompanied by a degree of flattery from the fake executive. Once the first payment has been made, the fraudsters will often return again and again until the fraud is discovered, by which time they may have got away with many millions of pounds.

Shutting the gates

Preventing this type of crime from succeeding is both a technical and management issue. On a management level, properly vetting temporary staff is essential. It is noticeable that those companies most commonly affected by this type of crime are those with seasonal recruitment needs, who are less able to run comprehensive checks on potential recruits due to the large influx of temporary staff at particular times of year.

It is also important that permanent staff, especially those employed in key areas such as accounts and procurement, are made aware of the potential for this type of crime and to be aware of the behaviour patterns of 'embedded' fraudsters.

If staff do suspect that something is awry, then it is important that effective whistle-blowing and incident response procedures are in place for suspicious activities so that staff can communicate their concerns to senior management. Some company cultures are more hierarchical than others and it is important that staff are able to report suspicions beyond their line manager and are not in fear of repercussions if they do.

"IT departments need to effectively control BYOD users, especially temporary ones. This may mean banning temporary staff from using their devices on company networks"

With access to computers, mobile phones and the Internet, the means of perpetrating these kinds of fraud are more available than ever if the right controls are not in place. It is also good management of temporary staff to limit their physical access to sensitive areas of the business such as finance and to limit their access to the IT system and documents to the minimum necessary. The duties of temporary staff should be segregated – do not allow temporary staff a wide remit.

The risk of fraud has been exacerbated by the growth of 'Bring Your Own Device' (BYOD) on many company networks, which increases the potential risk significantly. IT departments need to effectively control BYOD users, especially temporary ones. This may mean banning temporary staff from using their devices on company networks or at least the development of strong effective policies before any problems arise to ensure that the IT team can gain access to personal devices. Data protection and privacy laws make gaining access to personal devices very difficult after the event if the company's policy is not communicated to and agreed with employees in advance.

In respect of emails, IT departments can also set up systems to authenticate real email addresses and identify fake emails by implementing technical solutions that check certificate, headers and reply-to addresses. Security software is available to identify and quarantine spoofed emails and to provide legitimate sources of email with certificates that prove their authenticity.

It is quite common for spoof emails to instruct the recipient to reply to a different email address and staff need to be made aware that this may be fraudulent behaviour. Moreover, once email chains leave the company's own domain, investigating email communications becomes more challenging, especially if the email host is in a remote jurisdiction or if anonymising techniques have been employed. Some fraudsters use encrypted email providers which can make investigations harder still and legal action will often be required to access email trails.

Above all, once policies and procedures are in place, it is essential that they are adhered to. Confidential payments should

not be made, regardless of who apparently orders them. An embedded fraudster will quickly pick up where the weak links in the chain are to be found and will exploit them ruthlessly. However, all too often companies fall short of their own policies, leaving them vulnerable to fraud and misbehaviour of all kinds.

Action stations and security readiness

Incident readiness is critical if the damage caused by this type of fraud is to be contained. The fraudsters will have completed much of the preparatory work well in advance so once the actual fraud begins, it can be completed very quickly. Without a clear plan in place, therefore, delays in identifying the source of the fraud and allocating roles to key staff to deal with it can lead to serious financial – and reputational – risks.

The response to an identity fraud of this kind involves data identification and evidence preservation, including audit logs, server files, emails and backups. It also requires the company to identify which devices the individuals involved have used and whether any potentially relevant evidence has been encrypted, whether it is data assets, files, or more crucially, communication channels between parties. It is also important to know where data protection or privacy issues lie, especially if the company is a multi-national one, and whether legal advice will be required to facilitate accessing employees' emails and other information held on their devices.

After forensic preservation has been performed, analysis techniques can then be deployed to evaluate whether the employee(s) concerned was complicit in the fraud or an innocent party. This will also include determining whether malware has been introduced to the user's machine. It is then important to ascertain the chronology of events and to identify how the fraud was perpetrated to prevent it escalating or happening again. For companies to undertake this exercise successfully, they need to know – in advance – where their data is located so that they can begin the analysis as quickly as possible. In our experience, however, many companies do not have a clear idea of how their corporate information is disseminated, whether it sits in servers or personal devices, in which jurisdictions it is located and, increasingly, which elements of it are in the cloud. All can have a serious bearing on the ability of companies to effectively respond to an incidence of fraud.

However, many organisations may fall at the first fence. According to a survey of 316 companies worldwide conducted last year by Control Risks in conjunction with the Economist Intelligence Unit (EIU), more than a third of global businesses did not have an investigation response plan in place that would enable them to identify and retrieve vital data.

Companies need to address all these issues given the number of existential threats from regulators, anti-bribery laws and big ticket legal claims. Failing to have robust response plans in place will have serious ramifications in the event of a problem occurring. An added complication of impersonation fraud is that it is not always clear at the outset whether the impersonated executive really has committed the offences or whether he or she is the unwitting victim of the fraud. Investigating senior members of the management team can be an intimidating process for more junior members of staff and key questions may not be asked.

In these situations, external consultants will often be required to provide an impartial view as well as managing the investigation process in a technically and legally efficient manner and liaising with law enforcement agencies and regulators if that becomes necessary.

About the author

Ching Liu is practice leader for digital forensics at Control Risks (www.controlrisks.com). He has worked in cyber forensics since 1995 and has been involved in numerous civil and criminal cases involving computer fraud and misuse. He frequently assists law enforcement agencies and law firms on assignments including focused interrogation of computers on subject matters involving money laundering, terrorism, paedophilia, drug trafficking and murder. He has been involved in the investigation of high-tech computer crimes, such as on-line counterfeiting and electronic espionage.

How to reduce the risks of temporary staff

- Ensure that temporary staff have been properly vetted either by your company or the recruitment agencies that supply them.
- Make key permanent staff aware of the potential for this type of crime and alert them to the behaviour patterns of 'embedded' fraudsters.
- Establish whistle-blowing mechanisms to enable suspicious activities to be communicated to senior management. For this to be effective, it is essential that staff are able to report suspicions beyond their line manager and are not in fear of repercussions if they do.
- Don't allow temporary staff a wide role that will enable fraudsters to gather comprehensive information about the organisation.
- Limit the access of temporary workers to the company's IT system. Prohibit or restrict the use of own devices on company networks by temporary workers.
- Install security mechanisms to authenticate company emails and to identify and quarantine 'spoofed' emails.
- Prohibit the authorisation of any payments outside of the company's usual controls to all staff, including the most senior.
- Initiate a system of compliance to ensure that these policies are adhered to.