ComputerWeekly

Inside jobs – the security risks from the rise in temporary staff

Ching Liu

The growth in temporary workers is leaving companies vulnerable to a new kind of identity fraud - executive impersonation

One feature of recent economic times has been the rise in temporary staff. According to the Chartered Institute of Personnel and Development (CIPD), 29% of new recruits in the UK are employed on a temporary basis. Their numbers and their range of responsibilities are growing rapidly. While there are many sound management reasons for doing so, this is leaving companies vulnerable to a new kind of fraud - executive-level impersonation.

Individuals at companies are bombarded with spam or spoof emails and other, often unsophisticated, attempts to elicit fraudulent payments or install malware in their systems. Organised criminal gangs employing executive impersonation techniques can take this one large step further.

By embedding fraudsters in the targeted company as temporary workers to gather information, it ensures that subsequent attempts to extract money from the company are much more convincing and likely to succeed.

Once inside the company, the fraudulent temporary worker will attempt to find out what the company's payment protocols are and how they can be circumvented. He or she will also try to gain valuable information about the culture and organisation of the business.

To do so, they will often deploy "social engineering" techniques, such as getting friendly with key people in and out of work hours; and identifying a member of staff - often in the accounts team - most likely to unwittingly comply with fake requests to make payments or settle fake invoices.

Damage limitation

When a company becomes aware that something may be amiss, time will be of the essence. Given the groundwork that the fraudsters have done in advance, they will be a position to extract significant amounts of money very quickly once the second stage of the plan is put into effect. Delays in identifying the source and modus operandi of the fraud could be very expensive.

To counteract this - or indeed any other - act of fraud, it is essential to have an incident response plan in place. But companies often do not have such a plan, as a survey – conducted by Control Risks in conjunction with the Economist Intelligence Unit – found last year. The research found that a third of the 316 companies worldwide that took part did not have an investigation response plan in place, leaving them exposed to frauds of all kinds, as well as damaging their ability to react to regulatory interventions and large-scale litigation.

The key elements in the response to an apparent instance of fraud requires a company to identify and preserve evidence of the fraud - including audit logs, server files, emails and back-ups - which can then be subjected to forensic analysis techniques, to evaluate how the fraud was perpetrated and how it can be prevented from escalating or happening again.

To do so requires an organisation to have a firm grasp on where its data is held and to identify which devices the people involved have used. Depending on the legal jurisdiction in which it resides, data protection and privacy laws may

impede the company's efforts to access information held on personal devices, requiring legal advice - and perhaps court orders - to be obtained. Encrypted data may need to be circumnavigated quickly to locate evidence. Company procedures should also be in place to allow this to happen for an incident response case.

Allowing temporary staff to use their own devices on company networks is particularly risky, as is allowing temporary staff to use assets that are not properly locked down
A prickly additional problem in the event of impersonation fraud is working out whether the impersonated personnel is an innocent victim of the fraud or actually involved in the crime. In these situations, external consultants will often be required to provide an impartial view as 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.

Prevention and awareness will reduce risks

As ever, prevention is better than cure and there are a number of steps that an organisation can take to ensure that they do not fall victim to this emerging kind of crime.

First, ensure that proper background checks are performed on all temporary staff before they join the organisation and ensure they are not given too much physical or virtual access to key parts of the company's premises or systems when they join. Allowing temporary staff to use their own devices on company networks is particularly risky, as is allowing temporary staff to use assets that are not properly locked down.

Key existing staff should be made aware of the risk of this kind of fraud and the patterns of behaviour that may accompany it. There also need to be robust reporting mechanisms in place for any suspicions to be relayed to senior management which can bypass line management structures if need be and protect staff from repercussions if they make a report.

Security systems should be implemented to authenticate communications, identify and quarantine fake emails as they arrive. It is often the case that fake emails instruct the recipient to reply to a different email address, usually for "confidentiality" reasons.

Executive impersonation fraud is driven by financial gain. So, it should be made clear to all accounts staff that the company's controls on payments should not be circumvented in any circumstances, regardless of who is making the request. If this policy is strictly adhered to, the risk of CEO impersonation is significantly reduced.

Ching Liu is practice leader for digital forensics at Control Risks.