‘Ghostbusters required’: protecting organisations against huge potential fraud losses caused by ghost employees

By Rainer Jeske, Consultant at Datacentrix

A number of key South African organisations are potentially incurring significant losses due to 'ghosts' – that is, ghost employees, who exist on paper within business or government departments, but not in real life.

This issue is criminal rather than paranormal in nature, whereby ghost employees are one of the most prevalent types of occupational fraud, perpetuated through illicit payroll activities, and potentially resulting in substantial losses for the organisations concerned, whether at the level of a business or government entity.

And South Africa is not isolated in battling against this type of payroll theft: there have been many instances reported across Africa and even further afield, including the discovery of more than 80,000 ghost workers in the Nigerian police force; 30,000 on the Mozambican government payroll; and ghost employee scams also taking place within Zimbabwe and Kenya. Ghost workers are not exclusively a challenge for the public sector either; large organisations with diverse environments can be just as vulnerable.

To mitigate the risk and to protect organisations, leaders are needing to invest in technology that is capable of accurately defining positive identity, thereby ensuring transactional validity, assuring trust and data integrity, and enforcing accountability.

> Datacentrix's eDNA solution follows an authentication and trusted data management process to ensure that an organisation's individual identities and data are secured.

The Association of Certified Fraud Examiners (ACFE) is the world's largest anti-fraud organisation, with more than 90,000 members. In 2022, a global fraud study by the ACFE found that payroll fraud resulted in substantial financial losses overall, and that the presence of ghost employees was a key element of payroll fraud[1], accounting for nine percent[2] of reported cases globally.

The ACFE report notes: “Try as they might, organisations cannot prevent all fraud; if an organisation is operational long enough, eventually an employee will commit fraud. Consequently, the ability to quickly detect fraud is crucial. Our research indicates that the median duration of fraud – that is, the typical time between when a fraud begins and when it is detected – is 12 months. Additionally, the longer a fraud remains undetected, the greater the financial loss.[3]”

How do ghost workers enter the system?

Ghost workers, who are fictitious employees loaded onto payroll and business systems with the simple goal of defrauding the organisation or committing a crime, can enter the system through a variety of methods. These include being loaded or left in the system by corrupt employees, or introduced by threat actors looking to do more than just defraud the payroll.

Many government institutions battle with the ongoing ghost employee challenge as they manage a vast network of databases, systems and computers that do not adhere to the highest level of data integrity. Tracking the ghosts is a daunting task, and that's assuming that the business even knows that they are there.

For public sector organisations and large businesses around the world, it is imperative to create a comprehensive integrity management system, effectively managing and overcoming the challenges around counting employee heads accurately, and ensuring that there is comprehensive visibility into the complexities of ghost employees, duplicate records and potential insider threats.

So … who are you going to call?

'I ain't afraid of no ghost' is the saying in Hollywood, when the legendary heroes of the 'Ghostbusters' movies are called in – but these won't work as well in the digital world.

Instead, Datacentrix encourages organisations to consider a unique transaction security solution, such as its own eDNA identity and access management (IDAM) solution that institutes people accountability across all critical enterprise applications. This solution is designed to eradicate ghost employees and any other forms of fraudulent transactions from public and private entities, validating employees through a fool-proof biometric identification process. This would include forensically examining and assessing specific transactions to ensure that the DNA of the payroll and other critical applications' activities are tied to a physical person, providing legally reputable evidence of every activity undertaken in the systems. This provides organisations with an exceptional additional layer of preventative security.

eDNA presents nine steps to trusted data

Datacentrix's eDNA solution follows an authentication and trusted data management process to ensure that an organisation's individual identities and data are secured in the following order:

1. Secure enrolment that is compliant with positive identity governance, POPIA and Electronic Communications and Transactions (ECT);
2. Three-factor digital authentication that uses biometrics, then a Public Key Infrastructure (PKI) certificate, and finally a smartcard;
3. A secure access gateway, where logon is only permitted via eDNA's three-factor digital authentication process;
4. Customer sensitive data transactions are performed that need to be secured;
5. Business rules are defined for tracking sensitive transaction data;
6. Transactions done with eDNA are signed and sealed at the data's source;
7. Using the basis of a business intelligence and alert system to build customer frameworks for business rule tracking and reporting;
8. The solution allows for the forensic production of legally accepted data evidence; and
9. A tamper-proof system that ensures all computing facilities adhere to an end-to-end highest security level data platform and ultimate data protection.

The prevalence of ghost employees reflects broader issues of corruption and unethical behaviour, which can produce negative effects within society at large.

As noted by Nigerian Professor of Accountancy, Emmanuel Ikechukwu Okoye: “Fraud has become one of the greatest threats to the world economy. It is a global problem, not only in terms of its impact on our major corporations and key financial institutions, but also its effect on smaller companies and the wider public who indirectly pay for the losses through increased costs of goods and services”.

Rooting out ghost employees – and ensuring that systems are in place to make sure that they stay banished – is therefore an imperative undertaking for any organisation.

[1] https://legacy.acfe.com/report-to-the-nations/2022/
[2] page 12 of the report
[3] page 14 of the report

For more information contact Elzette du Preez on edupreez@datacentrix.co.za