

A Spartan with a laptop

Why the future of fraud prevention might need to be a lean, mean fighting machine

A WISE PHILOSOPHER once wrote, “prevention is better than cure”. It’s certainly true for fraud, for which there is rarely a cure once it has happened. Which means that, instead, we must place all our focus on prevention.

There are endless reports of the tidal wave of fraud that has emerged, and will emerge, from Covid-19, so fraud prevention is at the forefront of everyone’s minds, right? The truth is, it isn’t. Organisations are in turmoil – budgets set in January are a distant memory, supply chains are under significant pressure, employees are on furlough (particularly those in classic control functions), and cash flow is critical. That means investment in traditional back-office functions is minimal. Businesses don’t usually spend money on prevention in times of crisis – not when they’re struggling to pay staff and suppliers.

Contrast that depressing situation to the opportunity currently presenting itself to fraudsters – both those that have already stepped over the line and those who might be thinking about it. Normal control environments are in flux and unlikely to be fit for current operational purposes, traditional control functions are at home and unable to get out into the field, emergency funding is being issued rapidly and without the usual checks and balances, and supply chains look markedly different to how they did just six months ago. This all makes the perfect recipe for a significant increase in fraud.

So what are we seeing wise corporates do now to protect themselves, and what should they be doing in the future? The answer is, be proactive, and don’t place all your eggs in one basket.

Making fraud prevention a company-wide responsibility

Any fraud prevention system is only as strong as its weakest link, and that is invariably people. As such, clients are extending fraud risk management beyond the usual control functions and leveraging the three lines of defence. We are seeing companies implement a range of key measures, including:

- Educating employees on the latest fraud trends, and providing practical advice and examples to help them remain aware and alert. This improves engagement and prevents people from zoning out during the usual annual online training they often try to complete as quickly as possible
- Designing tailored control frameworks, that account for jurisdictional anomalies and cultural nuances, to ensure that the



Howard Cooper and Zoë Newman are managing directors and co-heads of financial investigations at Kroll, a division of Duff & Phelps



“We’ve seen many corporates lose millions to fraud, and then spend further millions trying to recoup what they’ve lost, when an insignificant upfront investment in fraud prevention would likely have detected the issue”

control environment is adapted to changing circumstances and environments, as opposed to a one-size-fits-all control policy

- Involving internal audit in the fraud prevention strategy. This invaluable and often overlooked function has some of the best and most hands-on knowledge of how the control environment works in practice. As such, auditors can provide informed advice to the design of fraud prevention mechanisms

Smart data analytics

“It would have been so obvious if anyone had looked,” is a phrase we hear time and again in fraud investigations. The problem is, very few do. If people are the weakest links in fraud, then why does the majority of fraud prevention rely on them?

Savvy corporates, those that truly understand that fraud prevention is a cost-saving in the medium term, have deployed sophisticated data analytics, running bespoke algorithms that mine the information available to them internally, within their financial and non-financial internal systems to spot anomalies at headquarters, but also around the world, in their most far-flung operations. No one knows this “live monitoring” is happening beyond a select few, who can use the results to spot red flags and dive into the data to assess the true extent of a potential problem, or a simple false positive. These “Spartans with

a laptop” can sit anywhere in the world, and do the work of tens of auditors at the push of a button. Big data is the future, but the ability to sufficiently understand your business to design appropriate queries to interrogate it sophisticatedly is what smart corporates are doing now.

Live risk assessment

Risk assessment has become something of a buzzword over the years, and frequently addresses business risk as well as bribery and corruption. The danger is these exercises become rote, and desktop focused. Only a few properly invest in well-thought-through fraud risk assessments, that are live documents. The reality is all risk assessments should be live, but ever more so in the case of fraud. All too often the risk focus is around cyber-security and the external threat, or an errant employee eliciting funds from the company – your typical frauds, so to speak. Only a handful will properly assess how their operational business environment has changed in the past six months and how controls need to be adapted to take these changes into account. What of the risk of financial misstatement, for example, or postponement of costs – all initially well intended and not an obvious immediate loss to the firm but fraud nonetheless.

So what is the future of fraud prevention? We’ve seen many corporates lose millions to fraud, and then spend further millions

trying to recoup what they’ve lost, when an insignificant upfront investment in fraud prevention would likely have detected the issue before it became business critical. Who knows what the world will look like a year from now, but consider this: corporates are being attacked by organised criminal networks constantly, if silently. At the same time their defences are weakened – whether through cost cutting, or the simple and unforeseen operating environment we find ourselves in. The profile of a professional fraudster has evolved: they are creative, specialised, use technology and adapt to their operating environment.

The Spartans of ancient Greece created a focused fighting force, trained in the latest fighting techniques and capable, with a small army, of defeating a much larger enemy. Corporates should consider something similar: engage and invest in a chosen few to become fraud risk specialists, empowered to leverage the workforce internally and data externally, and keep abreast of the latest fraud trends, to become your corporate defence. By leveraging the data available to you internally, and mining it intellectually, those Spartans with laptops might just be your saving grace.

INDUSTRY VIEW

hcooper@kroll.com
znewman@kroll.com
www.kroll.com