Identify and prevent rogue trading

Detica NetReveal’s head of investment banking solutions, Laura Houston, explains how the new networked operational risk model can help to reveal fraud

Banks have invested a significant amount of time, effort and money into managing large programmes to implement the mandated regulatory changes in relation to managing operational risk. Unfortunately, control failures are still happening, as high-profile incidents at Société Générale and, more recently, at UBS have demonstrated. They prove that typical control environments are no longer sufficient to prevent incidents from happening.

Weaknesses and holes can exist in every control framework, and these can lead to abuse by accident and as a result of malicious manipulation with intent.

Finding what you know
The primary objective of a control framework is to find behaviours that are known to be associated with high-risk activities. In effect, they apply business rules that generate alerts when a known control is broken. Through the course of business as usual, these control rules frequently trigger on legitimate business practice, and so typically generate huge volumes of false hits.

It becomes very challenging for an organisation to quickly identify the true abnormalities and high-risk behaviours among the high volume of low-risk alerts – the age-old problem of trying to find the ‘needle in the haystack’. Furthermore, the time spent moving through this volume of alerts is significant and it soon turns into a process-driven approach rather than one that aims to proactively find the true risks early.

Searching for what you don’t know
Of critical importance in the struggle to detect fraudulent behaviour is the siloed nature of both the control framework and the product areas within an organisation. While a trader may cancel a trade, it may not be known that this same individual has repeatedly made cancellations, they have not taken annual leave in 18 months and they have been logging in at unusual times.

Control areas are disparate, the investigations are conducted separately and frequently the only knowledge shared is by word of mouth. How does an organisation begin to identify the unknown without the capability to understand the more complex, repeated and hidden relationships that exist across different product lines, trading functions and systems?

As banks create increasingly complex control models, rogue traders’ methods become more sophisticated. Determined fraudsters understand a bank is a potential collection of control holes and weaknesses that can be exploited and, as one opportunity is closed, they will look for alternatives. It appears that, in recent incidents, the traders in question exploited a broad set of weaknesses across various areas of the bank and employed behaviours they knew would allow them to operate undetected. Their activities did raise suspicions but, because they were isolated incidents occurring infrequently across disparate areas of the organisation, they were not considered significant enough to take further.

BAE Systems Detica, in conjunction with leading investment banks, has developed a sophisticated networked control model to challenge these current weaknesses, enabling banks to take an earlier and more proactive approach to identifying instances of fraud and abuse. This unique model transforms a bank’s approach to managing operational risk through the implementation of advanced technologies, with methods and techniques used that were originally pioneered by secure government intelligence and defence organisations.

The solution, known as Detica NetReveal networked operational risk model (NORM), gives banks the ability to automatically analyse transactional and control data from multiple internal sources, from the front and back office, and across siloed areas to identify anomalous patterns, hidden relationships and changing behaviours at a much earlier stage.

It offers significant efficiency gains through user-friendly investigation tools and significant reductions in false positives through more effective and sophisticated prioritisation, using the following techniques:

- Cluster and peer group analysis – this provides risk assessments of each employee using the holistic and cross-silo view created by Detica NetReveal, identifying individuals whose behaviour stands out from their peer group.
- Social network analysis – sophisticated fraudsters spread their activities across multiple products, portfolios and systems in order to operate ‘below the radar’. They utilise and collude with other individuals and external counterparties to facilitate their abuse. The Detica NetReveal NORM solution utilises social network analysis to link apparently unrelated data from across diverse systems to automatically construct suspicious network relationship models for immediate risk assessment and subsequent visual inspection.
- Unstructured data intelligence – analysing the content of ‘unstructured data’ contained in emails, documents and other messaging systems, providing an invaluable source of intelligence.

It is important to recognise traditional control frameworks deployed in current systems are based on reactive rules and models that largely describe ‘the fraud we know’. Sophisticated fraudsters understand and evade traditional detection. The Detica NetReveal NORM solution can transform a bank’s ability to manage its operational risk across the organisation by enabling it to proactively reveal fraud that was previously hidden.