#9: Fraud risk management 2.0 – what does the future look like?

Future fraud will rely on a combination of technologies, devices and methods

The probability of being defrauded depends on will increasingly depend on the following aspects:

The organisation's extent of technology adoption

Organisations with multiple processes that have been automated may be likely to have an increased risk of fraud depending on the area and context of automation undertaken.

The organisation's technology exposure

The convergence of IoT devices, machine learning and innovative text mining methods have made it easy for fraudsters to identify areas of vulnerability within organisations. Businesses with internet facing, web based, data driven models can be misused to manipulate information and mislead users.

The organisation's adoption of nascent technology

Most organisations tend to adopt multiple technologies for different processes, with each such technology being in a different stage of maturity. Often when interconnected, the relative immaturity of one technology when pitted against the maturity of another can result in security gaps, exposing the organisation to fraud.

The organisation's technology adoption process maturity

Many leading organisations tend to have established processes for change control, production roll-out, risk assessment etc. for relatively mature technologies that they use. However for new models, depending on the maturity of the technology itself, levels of standardisation can vary. Limited standardisation and corresponding inadequate change control can lead to possible misuse to facilitate fraud.

Click here, to download the complete survey report