Getting real about AI and financial crime

With financial crime on the rise, institutions are increasingly looking to artificial intelligence to help them get the upper hand. But with so much 'hype' around this technology, there's a big difference between tomorrow's *possibilities* and today's *realities*.

How, then, do companies take advantage of the tools and techniques available now, while preparing themselves for what the future might look like? This article busts some of the myths about AI, helps organisations assess how ready they are for, their 'AI maturity', and outlines a practical roadmap for success.

Current approaches to fighting financial crime are expensive, time-consuming and not working

Despite investing hundreds of millions in technologies and systems to fight financial crime, institutions are still struggling.

Yet the majority of financial services companies still rely on what could be considered 'traditional analytical models' to fight crime. These models tend to be based on black and white rules and parameters; for example, if a transaction is

In 2016, almost half (46%) of the companies that participated in our Global Economic Crime Survey said they had experienced financial crime in the past 24 months. And local firms seem particularly vulnerable: more than a quarter (26%) of Australian respondents said they had experienced money laundering, a rate significantly higher than the global average of 11%.
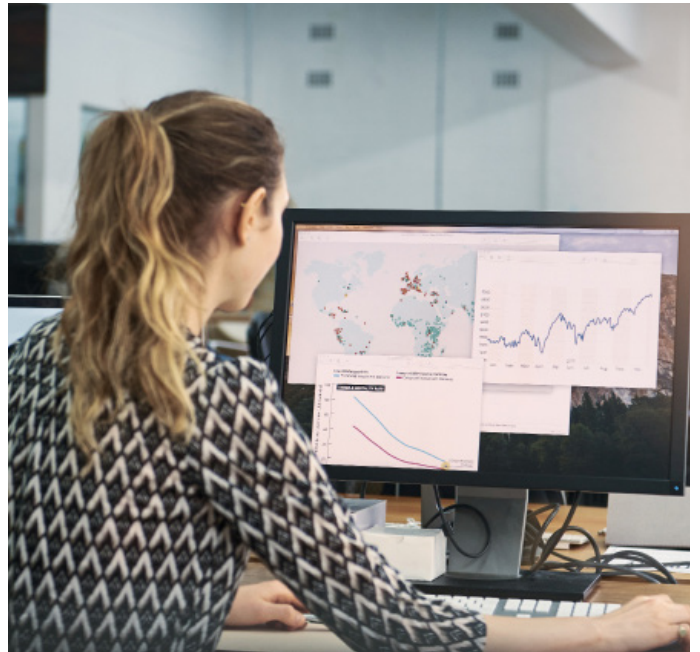
over $10,000 or a person uses a credit card overseas, then it gets flagged. The problem with simplistic approaches like this is that they tend to throw up an enormous number of false positives. And in an environment of increased regulation, increasing competition and increased cost pressures, it doesn't make sense to have your team trawling through thousands of alerts that don't represent real financial crime risks.

AI can help, but where do you start?

Most financial services companies are aware that artificial intelligence is getting faster and cheaper and offers a smarter way to tackle financial crime.

For example, AI can scan enormous amounts of data and identify patterns, behaviours and anomalies faster than any human can. It can analyse voice records and detect changes in emotion and motivation that can give clues about fraudulent activities. It can investigate linkages between customer and employees and alert organisation to suspect dealings.

But there's also lots of confusion about exactly how organisations should go about harnessing this powerful technology. Just because a certain technique is feasible doesn't mean that a company is in a position to apply it immediately.

To understand how your company can start to efficiently harness the power of AI, it's useful to dispel a few myths about it.

▶ AI is not 'plug and play'

AI is an umbrella term for the science that allows computers to do things that would typically require human intelligence to do. It can be applied to many things – from driving cars to playing chess to fighting financial crime.

But it's not an off-the-shelf solution that comes on a disk that you can install and get up and running straight away. Rather, it's an ecosystem of data and technology solutions; a combination of analytical algorithms, your data, external data and sophisticated software that must be tailored to tackle specific tasks.

So when it comes to using AI to fight financial crime, institutions will need to start small and then build out their capabilities as they learn and adapt.

AI is not new

Most of the mathematics and algorithms that underpin AI were developed in the 1970s and 80s. What's changed in the last few years is the explosion in computer processing power and the proliferation of data available to analyse.

For example, companies now have access to data from ever-expanding systems, devices, operating environments and sensors. And because fighting financial crime requires finding the proverbial needle in the 'haystack of data', AI has emerged as a particularly useful application to sift through the volumes of data.

You don't need 'perfect' data to use AI

Many companies are aware of some of the problems with their data's quality, and some believe that AI will not work if their data is less than perfect.

While it's true that AI algorithms rely on data to work – given the performance of IBM's Watson on the game show Jeopardy was only possible because the computer had access to Wikipedia, for example – you can certainly start developing capabilities in AI with whatever data you already have.

Obviously, the better the data, the better the outcome, but poor quality data shouldn't be an excuse to avoid starting your journey to using AI.

✓ Most are still at the starting gate

Despite the power and potential of AI to fight financial crime, the majority of Australian financial services companies either haven't started using the technology or are just dabbling with it.

Part of the problem is that they don't really know where to start, or conversely, are thinking too far ahead to techniques that are feasible but not practical yet.

Most would be better served by focusing on what's possible over the next 1 to 2 years, rather than what AI could do 5 years down the track.

▤ A five-step plan to move forward

☑ AI is a journey – understand where you are by assessing your AI maturity (see AI readiness assessment).

☑ Don't bite off more than you can chew – develop a plan for the next 12-24 months.

☑ Start by understanding the 'use cases' – what are the things that need fixing and that AI can help with? This might be transaction monitoring or monitoring of correspondent banking, for example.

☑ Conduct cost-benefit analyses on your use cases then prioritise where you're going to deploy your resources.

☑ Pick small, tangible problems – refine your approach by piloting and testing.

☑ Make sure you're recording and evaluating results – you need evidence to build the business case.

AI readiness assessment

Pillar	Topic	Low maturity ◄┈┈┈┈┈┈► High maturity	
Purpose, Vision & Strategy	**Do you have an AI Strategy?**	No analytics strategy	Clearly articulated analytics strategy incorporating AI aligned to both the Enterprise and IT strategies
	Does your organisation have a data-driven culture?	Gut instinct is often relied upon to make the right decision	Executives always seek evidence to support decision making
People & Organisation	**Is there an AI Operating Model?**	Unclear which analytics team to speak to or how the teams work together	Clear delineations of the purpose for each team with agreed handovers between each
	Do you have the right skills?	Staff skills and experience align to more traditional data analytics approaches and do not align to the AI technologies being used	Staff are re-skilled as required to hold deep skills and experience in the dominant AI technology and techniques being used
Partnering with the Business	**Establishing a pipeline of high priority use cases**	The AI team(s) decide what projects they are going to work on by themselves	A strong pipeline of use cases is constantly being curated with regular review from senior leadership teams agreeing the priorities for the AI team(s)
	Engaging with the Business and generating buy-in	Lack of communication throughout project delivery with lots of change requests required at the end, often resulting in the project ending without any demonstrable impact on the business	The business and key stakeholders are constantly engaged throughout the delivery of AI projects and they own the outcomes, with the projects having measurable business impact
Analytics Execution	**Operating to an AI analytics process**	Each activity has a "once-off" way of working that is different each time and depends on the person/team working on it	Every AI use case is executed according to the same standardised process with common activities, deliverables and milestones
	Standardising work products to increase re-use	AI datasets and code is not created to a consistent set of conventions or made available to others in the organisation	Data assets and IP are centrally stored, quality reviewed and made available for re-use by others in the AI/analytics community
Data Assets	**Access to data**	It is a time consuming process to constantly seek permission to access different data sets, the AI team can't get access to everything required and often only gets "once-off" copies of data dumps	The AI team has timely access to both structured and unstructured data sources to explore use cases, with common data sources "gold plated" and shared with other teams
	Integrated data	Most data is analysed in isolation and rarely integrated with other data sources – no external data is used in the analytics	Integrated data sets are pre-prepared for mashing and modelling (where possible) and the AI team also leverages geo-demographic data, social media data and subscribes to other external data sources
Technology	**Tools**	The AI team only has a limited set of tools available and does not have permission or budget to try new tools	The AI Team has a dedicated environment where new tools and techniques are encouraged to be trialled on different use cases
	Platforms	Does not have an enterprise grade analytics platform, currently working off people's laptops or on isolated servers	The AI team has multiple connected analytics platforms used by different teams, including "sandpit" environments as well as the ability to explore new technologies

Contacts

Peter Forwood
Partner
Peter.forwood@pwc.com
(03) 8603 0664

Phil Bolton
Director
Phil.bolton@pwc.com
(03) 8603 0408