Artificial intelligence: opportunity or threat?

Artificial intelligence (AI), also known as machine learning, is no longer the stuff of science fiction. AI has swiftly moved into mainstream awareness as technological advances and real world applications emerge at a faster pace than ever before.

A report by Bank of America Merrill Lynch forecasts that up to 35% of all workers in the UK and 47% in the US will be replaced by machines by 2025. This raises major concerns for the workforce and the skills that will be in demand over the next decade, and means businesses and non-commercial organisations must understand how their sectors will be shaped by this rapid change and, therefore, how they should respond.

No two sectors will be affected in exactly the same ways or to the same degrees. Jobs which require or benefit from deep interpersonal skills, such as counselling or investor relations, as well as creative fields, from the arts to sciences, are expected to be resilient to change, at least for now. Instead, it is tasks that are considered to be routine and repetitive, and therefore can be learned by a machine, that are most exposed.

PwC has said that in the UK 2.25 million jobs are at high risk in wholesale and retailing, 1.2 million jobs are under threat in manufacturing, 1.1 million in administrative and support services and 950,000 in transport and storage.

In the transport space, self-driving cars are already being trialled in cities around the world, including London, with automakers such as Nissan hoping that such vehicles will be commercially available by 2020. The rate at which the cars are adopted by consumers remains to be seen, but the commercial implications of obsolescing human drivers are obvious. For one, ride-hailing firm Uber has agreed to acquire up to 24,000 driverless cars from Volvo, while Amazon is investing in the field as it looks to own more of the value chain by cutting courier services out of delivery. Keenly aware of this imminent shift, car manufacturers are also investing heavily in driverless technology and repositioning themselves, as Volkswagen has done, as 'mobility suppliers'.

There is an understanding that the ability to successfully exploit AI will put companies in a strong position over the next decade and more. A survey of global businesses by Statista found that 84% believe investing in AI will lead to greater competitive advantages, and 75% believe that AI will open up new businesses while providing competitors new ways to access their markets.

It is imperative, then, that organisations understand their place in an increasingly AI-led world and the extent to which adopting machine learning represents an opportunity and, conversely, failing to do so represents an existential threat.

While internal audit has historically provided controls-focused assurance, there is increasing value in audit, as a trusted and independent adviser, giving an informed perspective on the extent to which risk is being managed outside of rigid controls and processes. Internal audit should be able to understand the risks and opportunities that impact on the organisation's ability to meet its objectives, and AI is no exception.

These are just some of the sectors expected to be most affected by automation and AI and, therefore, senior management in these industries should be thinking about the organisation's strategic approach to

this rapidly evolving technology:

Automotive and transport

Driverless technology is one of the most advanced areas of AI and self-driving cars are expected to be commercially available within three years. This has huge implications for car manufacturing, ride-hailing and public transport, haulage and logistics and many other industries.

Finance

Bank of America has already begun trialling automated exchange traded funds (ETFs), while independent financial advisers (IFAs) are expected to become obsolete as machines can build consumers' risk-adjusted investment portfolios. The financial applications of AI are expected to be numerous, from fraud detection to expediting motor insurance claims as computers learn to assess collision damage.

Manufacturing

Factories were the first places automated robots had commercial applications. As the technology advances, manufacturing will become more efficient as processes are refined and demand through the supply chain can be more accurately monitored and predicted.

Retail

Retailers are beginning to use machine learning to predict customers' orders in advance, in terms of what they are likely to buy and when. The customer experience is expected to be increasingly personalised by AI.

Healthcare

There are various ways in which robots and AI could be applied in healthcare, from diagnosis to treatment to end-of-life care. Researchers from Houston Methodist Research Institute in Texas have already developed a programme that interprets mammograms and translates patient data into diagnostic information 30 times faster than a human doctor, with 99% accuracy.

Professional services

Paralegals and other support staff are expected to be replaced by AI, as programmes can sift through huge volumes of information and data that would have historically been done manually. There are obvious benefits for large audit and accounting firms who can use AI to rapidly and accurately process financial data and inventories.

Due warning

"The pace of progress in artificial intelligence is incredibly fast. Unless you have direct exposure to groups like Deepmind, you have no idea how fast - it is growing at a pace close to exponential. The risk of something seriously dangerous happening is in the five-year timeframe. Ten years at most," warned Elon Musk, the CEO of electric car maker Tesla, in 2014.

A true visionary of our age, Musk has been one of the loudest voices regarding the threats posed by AI. But he is not alone. A recent report by 26 of the world's leading AI experts outlines the dangers that automated

technologies could pose, and they are not limited to the digital world.

The report notes that AI could be used to automate physical attacks with drones or to subvert systems that rely on AI, such as intentionally crashing self-driving cars. Few organisations outside of the military and self-driving vehicle and technology developers will be managing the risks associated with possible drone and other physical attacks, but AI also presents a huge digital security threat.

Today, organisations are investing more time and resources than ever into robust cybersecurity defences and protocols. This will need to continue since machine learning is likely to be exploited to carry out attacks. For instance, it is envisaged that spear phishing – an effective but time-intensive act of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information – and other automated hacking may soon be carried out by programmes. There is also the potential for data to be intentionally poisoned so that AI systems malfunction or give erroneous outputs.

This means that cybersecurity strategies and protocols will have to be agile and fit for purpose as the nature of the threat becomes more sophisticated.

AI and IA

Internal audit may not be a machine learning subject matter expert, but the function can add genuine value by providing assurance that the organisation has a well-informed AI strategy in place, and that associated risks and opportunities are understood and being appropriately managed and acted upon.

The following are questions that internal audit should seek to answer as such technologies continue to move into the mainstream:

- Is management thinking about the threats and opportunities posed by AI, both generally (e.g. sector exposure) and specifically (e.g. applications that apply to the organisation itself)?
- Has a risk assessment been carried out to determine the extent to which AI could prevent the organisation from reaching its strategic objectives, but also enable it in doing so?
- If yes, what is the conclusion of that assessment and is a strategy in place to mitigate those identified risks and exploit the opportunities?
- Has that strategy been clearly articulated to AI developers and project managers within the organisation, and other relevant stakeholders, and to what extent has it been put in motion?
- Are AI projects already underway and how well managed are they (e.g. objectives and delivery schedules)?
- Is there a clear view of the return on investment (RoI) achieved by past technology-related projects? That is, how successful have previous pilot projects been and have any governance weaknesses identified in those been addressed?
- The outputs of machine learning systems depend on unbiased, accurate data inputs. Are the risks associated with human error and poor or biased data being managed?
- Do the organisation's data policies, management and architecture (e.g. data lakes) support its AI objectives?
- If AI is already in place, to what extent is it fulfilling its strategic objectives and what risks does it present (e.g. security weaknesses or harmful outputs)? Have key risks been identified and are they being effectively managed?
- Is cybersecurity risk being appropriately managed and are cyber governance and controls sufficiently

agile to keep up with the potential rise in sophisticated, AI-powered hacks (e.g. mass spear phishing?)

Dr Nicola Millard, head of customer insights and futures for BT Global Innovation, weighs up the positives and the negatives of AI.

Further reading

PwC: Sizing the prize - What's the real value of AI for your business and how can you capitalise?

PwC: Will robots steal our jobs?

The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation