What CFOs can expect from technology's rapid evolution

---

1. Almost half the CFOs we surveyed have increased their investment in cybersecurity in the last year

2. 37% aren't yet evaluating the risks or benefits of AI

3. 30% considered effective data capture to be their biggest tech challenge

---

Technology's pace of adoption is slower than managers would like because of implementation difficulties and resourcing, according to the Private Funds CFO Insights 2024. Aztec's Director of Data Will Relf and Chief Information Security Officer Steve Pikett explore tech's rapid progress.

The subdued response to technology's impact in Private Funds CFO's 'Insights 2024' survey underscores the disconnect between the speed of technological advancement and the often painstakingly slow process of effectively integrating new technology into a business. Often this is because businesses don't have the necessary expertise to implement new technology successfully. Given the fact that more than 8 out of 10 artificial intelligence (AI) and machine learning projects fail, managers need to lay the foundations correctly to successfully reap the rewards of what new technology can bring, and to avoid being part of this damning statistic.

Of the 114 CFOs we surveyed, only 17% said that new technologies such as AI

and machine learning were already helping them to be more effective in portfolio monitoring, while only 12% said that new tech had helped them to source investment targets. Just 11% said AI had helped significantly with back-office management, while of the other crucial operational tasks such as risk management, deal due diligence and performance analysis, 7% or less said they were seeing significant benefits from new technologies. Despite the small numbers, many of these areas have the potential to deliver much more real value, with solutions already being developed.

What tech should I be testing?

What stands out from the survey results is that many CFOs are still in testing phase with AI, with half saying they are evaluating use cases, while it's an even split – just over 10% each – between those already using AI and those who have decided to steer clear of it altogether, for now at least.

The reason for the delay among those who are either testing it or avoiding it, will likely be that they first want to understand how it would fit into their workflows, or they want a better understanding of the potential outputs. There's also a third who responded that they had yet to see any practical AI use cases at all.

Of the managers who are already embracing AI across private markets, there are a number of use cases we can reference. One large asset manager we've spoken to is using AI to help analysts research potential investment targets to determine if they reach certain ESG criteria. What would previously have been a protracted manual process was optimised by having AI do 95% of the work, with the analysts applying their expertise to interpret the results.

Another use of AI is its ability to analyse customer data more efficiently, to better understand trends and improve customer experience. For fund managers, improving the investor experience is one area already showing improvement and enhancement using AI.

How can you tap into current automation innovations?

Accessing the latest technology and ensuring you understand the technology inside out is important. What is equally critical is knowing what technology best suits your needs and the problems you're trying to solve, as well as how to integrate it into your architecture.

The two areas in which those surveyed are expecting automation to deliver the most efficiency to their operations is in data capture and portfolio monitoring, with almost 6 in 10 signposting these two tasks, while a third expect better results for deal analysis. 23% said they expect KYC/AML efficiencies to improve as a result of enhanced tech.

AI can also make better sense of the data fund managers are processing, and then presenting it in more efficient ways to aid portfolio management. We are working with our partners at Lantern to build on this capability.

Technology is also being used to develop KYC efficiencies, doing liveness checks and using AI to identify patterns in transactions to spot AML anomalies. Finally, Aztec Group is exploring AI computer vision and machine learning to elicit data from documents and notices to reduce the burden of manual data entry and deliver significant efficiencies.

How does a solid data foundation build tech success?

Data is the area where the biggest gains can be achieved, but also the area with the most pain points, including effective data capture, data quality management, discovery, availability, synthesising and more. Beyond these, ensuring your data is secure and that the myriad risks inherent in holding sensitive information are mitigated. This is supported by the results of the survey.

An example of this is a firm partnering with data experts to build a world-class cloud data platform, leveraging best-in-class technologies. A secure and scalable cloud data platform enables the curation of high-quality data, with modern data products developed to increase the efficiency and efficacy to serve clients. Upon this technical foundation other digital data products – visual and APIs – address the fundamental data wants and needs of clients and their investors.

The strategic steps to data curation, enhancement, and preparation are often downplayed or grouped altogether by organisations embarking on their AI journey. This is why more than 8 out of 10 AI and machine learning projects and initiatives fail, according to the Harvard Business Review, which is double the rate at which corporate IT projects failed a decade ago. Most failures cite poor data quality or availability. That is why building an advanced data platform and capabilities up-front ensures the best possible data is available to train the AI agents.

Among the CFOs surveyed, when asked what areas of their operations they expected to outsource more of within the next year, between 42% and 46% indicated they'd increase their outsourcing of IT and cybersecurity. The rewards of technology are always tempered with the risks, and this is why managers should prepare for both.

What makes cyber security so difficult?

Cybersecurity is not only an ever-growing concern for CFOs, but for investors too, with almost 9 out of 10 of the CFOs surveyed saying that having strong cybersecurity protocols in place is a back-office must-have for LPs. The survey also found that investors' due diligence processes are putting increasing pressure on back-office functions 'to a great extent' for a quarter of those surveyed, and when it comes to what investors want to know more about from funds, cybersecurity ranks third after valuation and compliance, and just a few percent ahead of IT.

With the constant threat of a cyber incident coupled with the challenges of finding – and keeping – skilled staff to manage cybersecurity, many CFOs are keen to outsource elements of it. While handing off the problem to an outsource partner is attractive, it is not without its difficulties.

For most organisations, a practical approach to cybersecurity outsourcing lies in the already established and mature practices at one end of the spectrum, and extremely niche activities at the other. We have seen many "silver bullet" vendors spring up in the market, offering protection from every form of cyber-attack – something a real cyber expert would contend is not possible.

What is a practical way to tackle tech?

These vendors are a suitable fit for a small firm with no in-house tech professionals and will plug many of their gaps in protection, but this can lead to a false sense of security. Larger firms are trying to skill up their experts with domain and industry knowledge to consider advanced and future threats and prepare for them. What works best is moving the mundane and repeatable work to mature suppliers focusing on a particular area. Most often a Security Operations Centre (SOC) providing constant monitoring and identification of threats and taking swift action to stop or isolate the threat is where outsourcing is most effective.

Monitoring a vast array of log events from all sources, analysing, and making sense of huge amounts of data fits the "do-it-at-scale" methods used by outsourcers. Adding expensive tooling across a range of clients also creates an affordable and scalable means to be more accurate and far faster than most in-house teams. If it is then supplemented by AI, in what is termed a Next-Gen SOC, the combination of highly specific analysis that is then acted upon by capable people is a powerful combination.

At the niche end of the spectrum are skills which are highly specialised and rarely needed by single organisations but frequently called upon across all businesses. Cyber Forensics, which collects and identifies the technical data left as a "trail" after a cyber-attack are an example. These specialists may be appointed by an insurer, or contracted by an organisation that has been attacked.

Selecting an outsourcer who is capable and will continue to remain so at the pace of change in cybersecurity, is far more than a cost vs. complexity equation. The outsourcers face many of the same issues as the companies looking to outsource. Outsourcing some of the aspects of cybersecurity makes perfect sense. Retaining in-house expertise to work alongside the outsourced service makes even more.

What is expected of outsource partners?

Among the 114 chief financial officers interviewed for Insights 2024, more than 7 out of 10 said they currently outsource some or all their operations. Of those who do outsource, better use of technology is where almost a third see their administrator improving, while just over a quarter expect their administrator to make further investment in skills and expertise.

Technology should simplify how you do business, and the good news is that there are plenty of ways to partner with experts to leverage technology and skills to optimise your efficiency and profitability, so that you don't have to figure it all out alone. Keeping abreast of developments in data management and analysis, as well as AI and machine learning, are just steps in the process, integrating these rapidly changing capabilities into your business offering safely – along with retaining the right people to deliver it – is how a partner who is already doing this for others, can support your business.

To discuss any of Aztec's technology innovations, please contact Will or Steve.