wealthadviser special report
www.wealthadviser.co

A Global Fund Media Publication | **February 2019**

# Software solutions for wealth managers 2019

**Wealth managers get digital** **GDPR spurs tech growth**

# In this issue…



wealthadviser

## Publisher


**Published by:** Global Fund Media Ltd, 8 St James's Square, London SW1Y 4JU, UK
**www.globalfundmedia.com**




globalfundmedia

# Wealth managers face tsunami of change in digital age

By Beverly Chandler

Long gone are the days when wealth managers sat in elegant offices in the more expensive part of town, decorated like gentlemen's clubs – all leather arm chairs, hunting prints and a small snifter at the conclusion of a meeting.

While this might still be what some people want from their wealth manager, and indeed can still find, most firms are realising that these days the truly wealthy want a digital solution to their asset management needs.

And the wealth management industry is proving quite slow in making this adjustment to its offering. A 2018 survey from fintech firm InvestCloud reported that the investment management industry is drastically under-prepared to cater to the digital needs of the next generation of investors – not only in the US, but also in the UK.

Their study, 'The State of Digital Investment Management: Adoption and Usage in 2018', revealed that the vast majority of wealth managers (68 per cent) know they need to improve their digital technology to survive.

And we aren't just talking the occasional email correspondence. Close to half of the investors interviewed used mobile apps to manage their investments and selected a wealth manager based on a firm's digital proposition.

InvestCloud's findings are supported by a boom in the search for chief technology officers (CTOs) at wealth management firms. Another survey, this one from administrative service providers Intertrust, found that 53 per cent of asset management professionals predict a surge in demand for board-level CTOs in the sector over the next five years as the challenge to find senior talent to leverage disruptive technology increases.

The biggest skills gaps, according to the study, are in artificial intelligence (AI), regtech and compliance, with 38 per cent of firms struggling to keep up with latest tech innovations.

However, change is slow to happen. According to this survey, only 18 per cent of wealth managers believe that by 2023 most firms in their sector will have hired CTOs with a mandate to drive strategic change, particularly by harnessing the benefits of technologies such as AI, blockchain and robotics. A further third (35 per cent) expect that a minority of firms will have done so.

The study highlighted the growing challenges faced by organisations exposed to a technology skills gap; four in 10 (38 per cent) of wealth managers admitted that just keeping up to date with the latest technology innovations was a challenge. The biggest skills shortages are in regtech and compliance (45 per cent), followed by AI (35 per cent) and cyber security (30 per cent).

For InvestCloud, which supports more than USD1.7 trillion of assets, their solution comes in the form of a mock periodic table of over 300 apps, each designed to aid wealth advisers digitalise their businesses, allowing various levels of entry, depending on the wealth manager's existing infrastructure.

And the drive to digitise has its own effect in consolidation within the wealth management industry. Andy Creak, EVP Business Development, at InvestCloud believes that over the next three years around 400-500 key wealth asset management businesses will choose digital partners, transforming their businesses from largely paper to a digital automated business.

But this development is likely to be more of a complementary thing, Creak believes.

And there is a wealth of evidence that investors still like a personal relationship with their money manager, they just don't want reams of paper to deal with. Efficient software in the mix frees up wealth managers to spend more time on building and developing a personal relationship with their clients.

Another study comes from Vanguard, who found in their 2018 Adviser-Client Survey, that traditional adviser businesses are using technology to become more efficient and competitive. Investment services such as investment report, rebalancing and asset allocation are being automated, allowing the adviser to spend more time on a personal relationship with their client, the firm says.

Gautam Samanta, Global Head of BFS at NIIT Technologies Limited is in an excellent position to view the changing landscape of wealth management business. Within the financial services sector, NIIT is primarily focused on asset and wealth management, working on 170 plus business processes with 1200 plus strong people who have deep domain experience.

Samanta describes the level of change in the wealth management sector, occurring at the moment, as a tsunami. Assets continue to grow on the one side but face significant headwinds, he says.

The strongest of those is a big change in customer expectation. People are used to digital experiences, he says, and they expect that level of richness of experience within their interaction with their wealth managers.

This is true of baby boomers onwards, while Millennials are 'digital natives' who have not known a world without digital services so truly expect a digital solution to their financial affairs.

Samanta describes the gap between the laggards in the wealth management world who haven't embraced technology as almost 'a digital emergency' because the gap is widening so fast.

A digital offering can take a wide range of forms for wealth managers. The growth and success of robo-advisers has been a bit mixed in the UK, but across other geographical areas they have proved to be successfully causing disruption and challenges to established players.

The robo-adviser firm combines a digital offering with competitive pricing, which makes them a strong challenge for gaining new business from all those digital natives, not enamoured of the paper report and the odd hunting print.

And beyond the practical application of digital tools to the investment part of the wealth management function, modern firms need to use digital tools, and increasingly AI tools, to fulfil their requirements for compliance and cybersecurity.

All of the studies reveal that firms who don't keep up with those functions are liable to underperform and face consolidation in an industry that is seeing a great deal of merger and acquisition activity.

Financial services firms feature in the top five industries spending the most to recover from cybersecurity breaches. This is partly because wealth management firms hold truly valuable data on individuals, personal information and financial information, but may well have fewer resources in protecting them.

Wealth management firms who don't take up the digital challenge are likely to face an uncertain future. ■

# Considerations for wealth managers to improve their technology stance

## Interview with George Ralph

Technology advances over the last few years have ushered in new tools and solutions for asset managers to improve how they streamline and automate their workflow processes.

Wealth managers have a big opportunity to evolve their business offerings in line with digital investor trends, and potentially steal a march on their competitors but to do so will require an open mind on how they think about technology risk and their ability to develop a robust IT framework; one that stands up to scrutiny in an increasingly complex regulatory environment.

A report by ***Fidelity*** entitled *How cost pressures will reshape the asset management industry*, states that asset management firms with complex layers between investors and their assets will lose ground to robo-advisors and other wealth management-type services.

The global robo-advisory market is forecast to grow at a annual compound growth rate of 53.54 per cent from 2018 to 2023, according to the ***Global Robo-advisory Market (2015-2023)*** report.

For any forward-looking wealth manager, technology innovation could result in significant revenue increases. This cannot be underestimated given that GDPR and MiFID II regulations in Europe, among other global regulations, are collectively placing huge margin pressure on wealth managers. A report by ***WealthBriefing***, for example, suggests that some 57 per cent of wealth managers believe that regulatory change will increase even further in speed over the next three years.

In addition, the report found that 49 per cent of wealth managers were "willing or wholly willing" to embrace outsourced hosted technology solutions.

**George Ralph, Managing Director of RFA**

This is good news for RFA, a leading technology consulting group which offers a comprehensive range of IT services to fund managers.

### Prioritising technology risks

As wealth managers embrace technology, it is paramount that they understand the risks in their operating models.

"At a top level, we conduct a site survey to assess what the client has in place, with respect to software system infrastructure, cybersecurity controls, etc," explains George Ralph, Managing Director of RFA. "We then follow that with a workflow review, which looks at the client's workflows from an operational perspective.

"From this, we identify the highest technology risks and advise the client to address them."

At the end of the evaluation, RFA puts together a recommendation report, which gives the client a full overview of what they need to do next and any products/tools it thinks they should implement to improve the efficiency of how they use their computer systems.

"We might recommend that firms bring in specialists from outside to help them with different areas of their business," says Ralph. "Our partner APS Solutions for example, are change management and transformation specialists in the wealth management sector. If we see a need for additional expertise to address risk in a clients' operations, then we have a network of experts we can introduce."

The introduction of general data protection regulation (GDPR) in Europe requires wealth managers (and indeed all European businesses) to keep their clients' personal data safe and secure. Those who fall foul of data breaches without having proper controls in place risk facing financial penalties up to 4 per cent of their total annual turnover.

"From a technology viewpoint, as wealth managers introduce new technologies and cloud systems it is making them more efficient as it allows investors to log on to see their portfolio allocations in real time, but at the same time it introduces more back-end complexity," says Ralph.

### Vendor risk

As wealth managers embrace outsourced technology solutions, one of the key considerations for staying secure is vendor management.

"More wealth managers are embracing, yet they don't necessarily have the in-house skills to do all the due diligence.

"Our clients are able to utilise us – many of whom are former CTOs – to do vendor management because we have the requisite due diligence skills. The risk management process we use extends through to vendor management, where we use a scoring system based on due diligence. A vendor like Cisco, for example, would be a low risk as they don't have to provide a system and organisation controls (SOC) report. However, if it is a cloud provider like Microsoft Azure, they have to provide annual SOC reports. We log whether we have to chase each supplier for the SOC report or whether they proactively provide it," outlines Ralph.

### Cybersecurity awareness

Various industry reports suggest that wealth managers are still lacking in confidence when it comes tackling cyber threats. But as they introduce more automation to their business models, wealth managers will need to get up to speed when it comes to building and maintaining a strong cybersecurity posture.

Ralph observes that one of the problems with GDPR is that a lot of financial institutions do not necessarily understand that the data processor is just as liable to pay the financial fines for a data breach as the data controller is. "I get the sense that many firms, however, still do not know what a data processor is. Any third party who has access to your data, including IT contractors, which a lot of firms use rather than full-time staff, is considered a data processor.

"We have an e-learning compliance training tool for all staff to use, including contractors, which allows senior management to review who has completed the training; it covers all aspects of compliance, from GDPR to cybersecurity," explains Ralph.

Last year, RFA was certified by GCHQ to do GAP analysis on GDPR, which was an extension of its existing cybersecurity audit. As such, RFA is fully certified as part of the IASME governance standard.

"We look at a client's data privacy impact assessment, data categorization, IT policies and procedures, all the way down to how they configure their firewalls and manage intrusion and detection," says Ralph.

### Artificial intelligence developments

One example of how RFA can bring artificial intelligence tools to benefit wealth managers and stay one step ahead of potential data breaches is a new intrusion detection and prevention monitoring tool, called MDR (Managed Detection and Response).

Rather than operating statically in a single environment like some intrusion detection systems, which are reactive and rely on humans to read the data logs to see if any suspicious activity has occurred on the network, RFA's solution proactively identifies any breach that may be occurring.

"One client tested this system alongside a couple of other high-profile software providers where the portfolio manager deliberately started downloading a series of spreadsheets. The two other software systems did nothing because they did not consider it malicious behaviour, whereas our system blocked his machine immediately as it was unusual behaviour," says Ralph.

### Practice makes perfect

RFA also conducts virtual disaster recovery exercises to test its clients' staff members, as well as investigative response work after an actual breach has happened, to help them identify what steps to take immediately.

"If you have to report a breach to the Information Commissioner's Office, they want proof that you understand why it happened and have put the right processes in place to stop it happening again. We recommend doing a disaster recovery test every year and that the client performs a virtual DR test every six months," concludes Ralph. ■