Fundipedia Blog

Is in-house software putting your asset management firm at risk?

If you have the budget, know-how and, yes, the fortitude to take it on — in software development, if something can go wrong, it's almost guaranteed to do so — building enterprise software in-house can seem like an attractive proposition.

But while there's no arguing with the benefits of getting it right — a completely bespoke, tailor-made platform that fits like a glove into your legacy infrastructure (and which you could potentially monetise) — there's an important question you should ask yourself before you get stuck in.

Is it worth the risk?

Admittedly, we're a bit biased. But we strongly believe the answer to this question should be a resounding 'No!'

In this post, we'll explain why in-house software often doesn't cut the mustard from a security perspective, and explain how working with a third-party vendor is a safer choice.

Gaming the system

You don't have to look too hard to find stories of firms whose software has let them down.

In 2015, for instance, a Morgan Stanley employee stole data belonging to 350,000 of the firm's wealthiest clients by exploiting a vulnerability that had gone undetected.

When the SEC investigated the breach, it learned that the software lacked effective access controls. In other words, staff who didn't need to (and weren't senior enough) to access sensitive data were able to view it, and, much worse, to copy and paste it.

The controls also hadn't been properly tested or regularly audited, so the issue wasn't picked up until it was too late.

Capital One got into similar trouble in 2019, when a hacker got their hands on 100 million customers' credit card details. Here, the culprit was an improperly configured application which enabled third parties to access data they'd otherwise never have been able to get to.

Most recently, in February 2023, Succession Wealth reported being the victim of a cyber attack.

The nature of, reasons for, and extent of the breach are still unclear. But security specialists have speculated that, based on what Succession Wealth has said so far, the breach might have been caused by unsuitable encryption.

We don't need to tell you that data breaches have extremely serious consequences for asset management firms, but we'll do it anyway.

Regulated firms have to comply with a long list of strict data security and privacy rules — GDPR, and regulator-specific rules such as those in the FCA handbook just to name two. So these breaches inevitably result in heavy fines.

The SEC fined Morgan Stanley $1 million (around £820,000) for the breach, for instance, while Capital One got fined an eye-watering $80 million (£65 million).

More to the point, research suggests that, when it comes to reputational damage, financial services firms have more to lose from data breaches than firms in other industries.

Consumers are less likely to be forgiving, especially if they think the response was slow or inadequate. And they're also more likely to stop doing business with the firm and to recommend that family and friends do the same.

Playing it safe with a trusted third party-vendor

There are many reasons why in-house software can underperform when it comes to security. But, in our experience, it typically boils down to two key factors: limited resources and a lack of the right expertise.

For enterprise software to be fit for use by asset managers, it needs to comply with highly complex technical requirements — on access control, on encryption, on vulnerability management, on disaster recovery... the list is endless.

And when your specialty is finance, not technology, it's highly unlikely that you'd have somebody on staff with the in-depth knowledge required to solve the very specialised problems that might crop up when addressing these issues.

Consider access control. If firms like Morgan Stanley and Capital One — Morgan Stanley, for instance, has over 80,000 staff — can get it so spectacularly wrong, chances are it's an even bigger struggle for firms with fewer resources at their disposal.

To make things more challenging, in-house software is typically hosted on on-premises servers. These need to be continually monitored, and may be vulnerable to internal attacks.

By contrast, because specialist third-party vendors are technology companies, not financial services firms, they have security baked in.

For one, their reputation depends on it.

As Oracle's VP of cloud security engineering Johnnie Konstantas has explained: '*Most providers ... have built the entirety of their business on the platform... As such, the protection of ... the infrastructure ... is priority one and receives commensurate investment.*'

Here, Konstantas is talking specifically about cloud service providers. But technology companies — whose entire business model revolves around being trusted by companies that have a lot to lose if the tech fails — adopt a similar attitude to their product.

Fundipedia's platform, for instance, is certified ISO 27001:2013 compliant: the gold standard for information security management. And an independent third party carries out regular penetration testing, so we can identify and fix security vulnerabilities before they can be exploited.

Technology companies are also free from the constraints asset managers have to contend with because of their reliance on legacy technology. They can build their software using a modern, standardised, more flexible tech stack. Which makes it easier to implement and maintain features such as high-end encryption at scale, than it is for an in-house team

Crucially, because third-party vendors serve a range of clients, instead of being focused on a single firm, they have broader visibility into common industry challenges.

This greater knowledge of the issues means they're better equipped to solve issues an in-house team would struggle with, such as how to make the platform comply with the differing regulatory requirements of several jurisdictions.

You can't afford to get security wrong

By 2025, it's thought $10.5 trillion (around £8.6 trillion) globally will be lost due to data breaches.

And because they sit on enormous amounts of highly sensitive data — personal details, financial details, and, more significantly, details of financial transactions — asset managers will be prime targets.

The good news is that most hacks — and the financial and reputational harm they cause — are avoidable. But security needs to be embedded into your enterprise software's DNA. And that's why the right third-party vendor is a safer bet than developing enterprise software in-house.

Think of it this way.

You wouldn't build your own house yourself, even if you were handy with a trowel and cement. So why risk going it alone, when a specialist vendor can make sure your software's foundations continue to be solid in the long term?

At Fundipedia, we've built a data management platform that's powerful, highly customisable, and, most importantly, meets the highest security standards.

Book a demo

Recent Posts

A Blueprint for FinTech Engagement and Onboarding in Investment Management
→
23rd April 2024

Fundipedia is recognised in the WealthTech100 list by FinTech Global
→
3rd April 2024

Getting the most out of your data and technology with managed services
→
13th February 2024

Navigating the new EET v1.1.2
→
8th February 2024

New year, new priorities in the evolution of data management
→
30th January 2024

+44 (0) 845 867 2845 | info@fundipedia.com
United Kingdom
8 Devonshire Square, London, EC2M 4PL
Luxembourg
9 Rue du Laboratoire, 1911 Gare Luxembourg