This document is for investment professionals only and should not be relied upon by private investors.

November 2021

Why cyber security is now a core concern for financial advice firms (and how to improve your protection)

FundsNetwork

Fidelity INTERNATIONAL

Introduction

In 2018, just 6% of financial advice firms considered cyber security to be one of the most important challenges to their business.

Source: Business challenges facing financial advisers.

Fast forward to 2021, and phishing, email scams and data breaches have all risen in prominence across the industry and in our individual consciousness. New working practices due to the Covid pandemic have changed the risk profile of many organisations, increasing the opportunity for cyber attacks. Financial advice firms are increasingly taking note.

TOP 3

Cybersecurity is among the top three business risks for large advice firms

Source: Nextwealth's Financial Advice Business Benchmarks 2021.

NextWealth's latest Financial Advice Business Benchmarks report shows cyber security is now one of the top four business challenges overall for advice firms and top three business risks for large advice firms. In fact, firms managing in excess of £500m of client assets name cyber security as their number one concern.

Contents

The cyber security issues facing advisers

The rise of the six percenters

Only 6% of firms considered cyber security a key business challenge three years ago – so what did they know that others didn't?

Often cyber security in advice firms was driven by someone bringing prior knowledge and awareness into the business. Alternatively, the firm employed a dedicated IT person, either on-staff or outsourced, who was well-versed in security considerations and able to articulate the importance of a cyber strategy.

> **"I would have been one of the 6%. We have had a cyber strategy in place now for five or six years. Security and being able to continue to run the business have been high on our list of priorities."**
>
> COO, wealth management firm

Given the general trend towards technology as the core of an advice business, whether in terms of the client proposition, technology infrastructure or security, the IT function is growing in importance.

> **"It's a mindset; an enquiring mind. People have a classic growth mindset to other areas, but not to IT. Every business now needs someone with this mindset to survive the next 20 years."**
>
> Financial planner

> **"I worry about our sector, we're a fantastic target for people who want to access customer data and people's money. We're untapped by the criminal classes by good luck."**
>
> Financial planner

Towards an inflection point

Some in the industry expect to see the regulator's stance on security move from guidance to statutory requirements for regulated firms – most likely in the form of self-certification for financial advice businesses.

Others forecast that a high-profile firm failure or a significant incident involving the loss of client data will be the inflection point that brings cyber security to the fore.

Despite the presence of cyber risk on advice firms' radars, many businesses may not be doing enough to protect themselves and their clients, this could be because tackling cyber security can seem daunting and expensive.

Bring cyber security out of the back room

"There is still a perception that this is a highly sophisticated area, really technical, really complex, and that is true of some very targeted high-profile attacks. But there's a wider recognition now that this is a more general risk that businesses need to manage. If you think about the basic things you can do, these will protect you personally and your organisation from the vast majority of opportunistic attacks. If you put in place the basic hygiene elements, which are free to do, you're going to put yourself in a much better position to protect yourself against this threat."

Adam Haylock, Global Head of Cyber Information and Security, Fidelity International

Do the basics and do them well

Certain key measures can be taken by all financial advice firms to address the biggest risks.

Embracing technology is a key factor. However, there are straightforward steps outlined in this paper that every financial advice professional can take to vastly reduce the information security risks to their businesses and clients.

The nature of the risk

"I'm flabbergasted by the low level of awareness. We are responsible for millions of pounds of client money. I see it as a basic client hygiene factor."

"It is a core component of what you've got to get right."

Financial planner

"We have just been through the Cyber Essentials process; very interesting and eye opening. We found (and fixed) many potential holes and risks in our little business, so I suspect many firms are oblivious to the potential and growing risks. We now prevent our computers from being used for personal stuff by all home-based staff and have software that flags any risky emails or downloads to prevent silly mistakes. I suspect many firms do not realise the danger their laptops pose."

Paraplanner

The Invisible Gorilla

In the classic selective awareness test, an audience is asked to watch a short video of two teams passing a basketball between players, and to count how many passes the team with white shirts makes. At the end, the audience has focused hard for the win and generally gets the answer near enough spot on.

What very few people see first time is that, midway through the video, a person in a gorilla suit strolls across the action, looks at the camera, thumps their chest and walks off.

Businesses may hear in the news and across the industry about cyber-attacks on company networks and many have technology solutions in place to help prevent and detect when they are being targeted however this form of deliberate or randomly generated attack may not be the biggest concern to organisations.

The biggest risk is the invisible gorilla. This covers areas which may seem obvious but could potentially be overlooked, things like the basic security controls or your employee base who are already part of the organisation and a potential target. In the financial advice industry, that might be someone in the firm printing off client information, or storing information on their personal mobile phone, or clicking a link in an email without being suspicious of its origins.

"It's not about having the strongest front door. You've also got to have the fire prevention policies, fire escapes and the fire-fighting equipment. You need to be able to roll back to a previous version of software if there has been a compromise. You need plans and policies in place, and you need to enforce them."

COO, wealth management firm

ii

The impact of Covid

For a number of reasons, the Covid pandemic has jolted information security onto more firms' management agendas.

1

A rapid and unplanned shift in working practices

"I think what we've seen with Covid is more people thinking 'when I was in the office, my organisation took care of security for me, now we're all at home'. I think it brought it to the front of mind for people who may not have questioned it before. They're sitting at home probably feeling a bit more vulnerable and wondering if the organisation is more vulnerable.
The answer to that is all the controls you had in the office still apply at home. There are some other risks, such as printing at home and so on, things staff may not have done when they were in the office. But generally, if organisations have secure VPN, encrypted devices, good monitoring, good endpoint controls, all this stuff that protects you in the office protects you at home."

Adam Haylock, Global Head of Cyber Information and Security, Fidelity International

"That's where policy and enforcement becomes so important. You can't just have a piece of paper that says employees cannot use company laptops for personal activities. You have to follow disciplinary procedures. No administrator accounts, so staff can't download their own software."

Financial planner

2 High profile security issues

Advice firms were quick to switch to video conferencing tools such as Zoom to collaborate with colleagues and meet with clients. Early on, it came to light that not all businesses had fully considered the security protocols that would need to be used to keep client data and conversations protected. Examples like these prompted firms to give more consideration to their information security.

3 Covid provided opportunities for phishing attempts

Phishing is a cyber attack which attempts to gather personal information or compromise technology for the purpose of financial gain or malicious activity. For advisers, the most common form of phishing is where someone poses as a legitimate organisation and sends a fake message by email, telephone or text in an attempt to persuade individuals to give sensitive data such as identification details, passwords or banking details.

"Cyber criminals are not stupid. As with any global event, they saw Covid as a massive opportunity. Phishing went through the roof – there were lots of hooks around Covid and the World Health Organisation, for example, so they were more successful. They had better content that people were more likely to click on. So, there was an increase in the number of infections, particularly for those organisations that didn't have good hygiene. They were able to get people to click on things, and that's generally how it starts. But criminals are also finding their way into organisations through vulnerabilities in remote access infrastructure. This is where it does get a bit techy. More companies are using more remote access and more security defects are coming to light. Cyber criminals are targeting these vulnerabilities."

Adam Haylock, Global Head of Cyber Information and Security, Fidelity International

iii

Five considerations for advice firms on the cyber security threat

1 People

Unfortunately, firms' employees are commonly the target for cyber criminals. This is because businesses are investing more and more in security technology to protect themselves from remote attacks and so the best way in for criminals is often through staff. It's therefore important that everyone within a firm understands their security responsibilities and follows simple cyber hygiene practices to protect the firm and themselves.

"The weakest link in a business is people. People clicking on links, people being coerced to do things and give away information; people behaving badly – printing client lists, holding personal information on their phones. What you need are lots of policies and procedures and staff training. It's part of our induction process for new staff, but you also have to keep it front and centre in people's minds. Log off properly at night, lock your screen when you leave your desk. We use software to randomly test our staff capabilities and remind them about cyber security every few months."

COO wealth management firm

"You can have the fanciest firewall, but the far bigger risk is the people in the business. You've got to have the policies in place, but also the enforcement of those policies."

Financial planner

CYBER ESSENTIALS

Advice firms can find a useful list of information security policies by visiting the NCSC website and following the Cyber Essentials checklist. **See page 13 for details.**

2 Dedicated responsibility for information security

We see an emerging trend for advice firms to bring the IT function in-house, rather than use an outsourced provider. This reflects the expanding role of technology in delivering the advice proposition. The IT role encompasses infrastructure, applications as well as security.

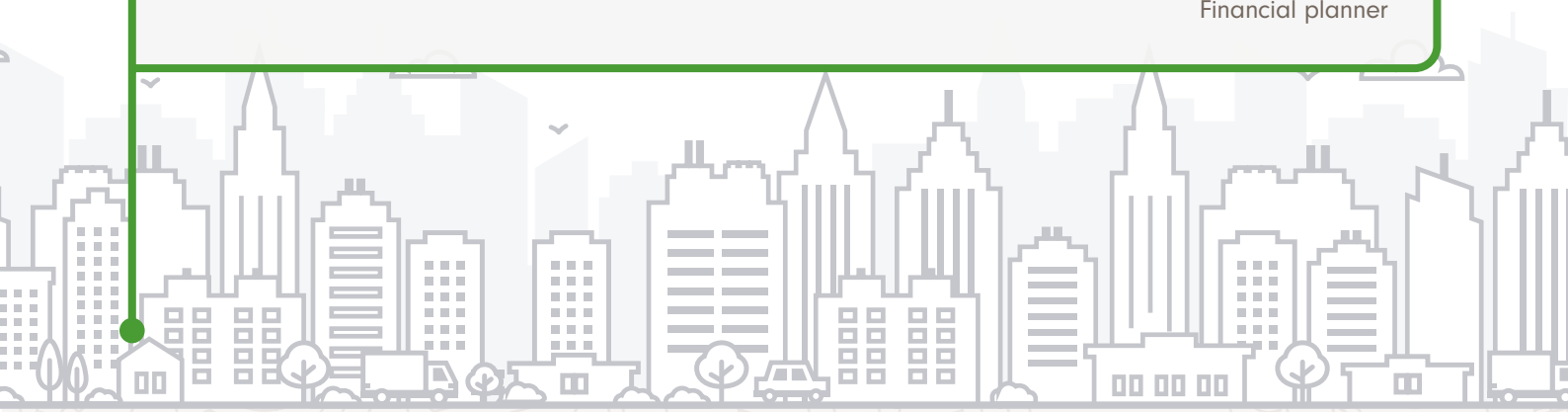
NextWealth's Financial Advice Business Benchmarks Report details the mix of staff found at advice firms of various sizes. Currently IT represents just 1% of staff hired, and one in five firms have an IT employee. In larger firms with assets over £500m, over half employ a dedicated IT person.

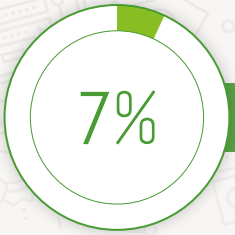
"Firms in our sector typically spend 6-8% of turnover on IT and that will only increase as we interact more and more with clients electronically. Last year we hired a dedicated information security officer who spends all their time thinking about security, maintaining systems, auditing our systems."

COO, wealth management firm

"Like many firms, we work with an outsourced IT department but we now also have a dedicated internal IT person. This is only a relatively recent thing. Two-factor authentication is now in place. I think a password manager is next on the list. The other thing that we do as a firm is work with an external risk firm called Risk Evolves. They talk to us a couple of times a year about phishing, or whatever it might be that's worth thinking through, so that we are quite up on it as a firm. It's front of mind."

Financial planner





Percentage of financial advice firms planning to hire an IT professional in the next year

Whether in-house or outsourced, firms should call on the expertise of their IT resource to regularly review and maintain security systems and software.

"We communicate with our clients about good practice and we've started talking to them about getting their own password managers. I'm genuinely thinking of making it part of our service, getting them set up and using LastPass or 1Password or another secure password manager."

Financial planner

3 Secure communications with clients

NextWealth's research indicates 70% of advice firms are now using client portals that offer the ability to securely communicate and share documents with clients. That's a 16% increase in the past two years.

Firms are also looking at tech in the client onboarding process to capture client details ahead of the first meeting. As well as streamlining processes and creating a slicker client journey, this has the added benefit of improving security.

Some firms are even considering advising their clients on financial data security as part of their role in looking after clients' financial interests.

"We work with Jotform to design secure online forms to capture clients' information via our client portal. Before we had that system up and running, I can think of a couple of occasions where someone said 'I'm not prepared to put that on a PDF and send it back because I don't think it's secure enough'. I completely understand that mindset."

Financial planner

4 Secure communications with providers and platforms

Covid also accelerated the adoption of paperless processing and eSignatures for many providers. In November 2020, NextWealth's research into the adoption of digital document submission processes named four providers as digital process champions; AJ Bell Investcentre, Fidelity International, Standard Life Wrap and True Potential, for digitally enabling 90% of their processes.

In some organisations, however, advisers are still having to send and receive client information by less secure means, including post.

There's client-to-firm, and we've put a lot of time into getting that bit right recently. Then there's firm-to-provider and we've got much less control over this because the provider is always the bigger beast in the relationship. We usually have to default to their systems instead of ours."

Financial planner

"Everyone approaches it differently; some providers have a secure system they want you to put data into but they can't allow you to pipe into them. They can seamlessly put barriers on doing things. It varies on the provider and their attitude. With Fidelity, for example, we have automatic links, two-way, secure and dedicated. We can provide information securely to them and them back to us, but the relationship has to be a certain level."

COO, wealth management firm

"I do think some of the technology and platform service providers have a responsibility to support some of the smaller advisers. So, if an advice firm is using a suite of products from a technology company or platform, then there should be more responsibility on that provider to ensure security."

"We see a lot of postal intercept fraud. We've really tried to digitalise everything and get away from post because it can be a problem. It also comes down to policy. How do you manage the physical information you've got? Have you got shredders at home? Are you making sure you're using them because if it goes out in the recycling bin, it's not beyond the realms of possibility that someone picks it up. You do need to be conscious of that."

Adam Haylock, Global Head of Cyber Information and Security, Fidelity International

5 Regulation and self-certification

Given the risk posed to both client data and business continuity by cyber security threats, some in the industry expect to see more regulation in this area, perhaps in the form of self-certification for advice firms.

"Operational resilience rules don't tend to apply to adviser firms at present, although this depends on the services they offer. In particular, the rules are currently unlikely to apply to smaller and medium-sized firms. However, given a cyber attack can have a huge impact on an advice firm, I believe the regulator will move from guidance to policy requirements at some point. For example, companies may have to self-certify and provide the evidence that they have done so. It could be to standards like Security Essentials."

Adam Haylock, Global Head of Cyber Information and Security, Fidelity International

"The FCA have done a number of surveys on information security and cyber security and provided feedback. I don't think they understand the landscape. It's a blunt instrument."

COO wealth management firm

"I'm not so sure they are well-placed themselves. Quite often the FCA's own email practices go against good practice. They come from a non-core domain and get picked up by our phishing filters."

Financial planner

Three steps to take to reduce business risk

Cyber Essentials

Visit the NCSC Cyber Essentials website and spend 30 minutes reading through the self-assessment criteria. The vast majority of common cyber attacks are looking for targets that do not have these criteria ticked off.

There are certification bodies who will assess your business against these criteria, or you can work through it as a self-guided process to ensure you have the basics covered.

Some of the criteria will need the verification of an IT person. However, a lot of the criteria are based around policies that you can put in place at your business.

"I would say 95% of the risk factors are reduced by completing this process."

Financial planner

"I always say to people, go to the NCSC website and look at the guidance for small businesses. It doesn't get any clearer than what's on there. They tell you where it's free. I'm very conscious that not all organisations have money to spend on this and they have to balance it against where this sits on their risk profile. Look at the guidance. It takes half an hour to read it. It takes longer to implement but if you just give that time commitment to do it, it's well worthwhile."

Adam Haylock, Global Head of Cyber Information and Security, Fidelity International

Enable two-factor authentication

Enable two-factor (or multi-factor) authentication in your financial planning tech. Two-factor authentication means adding a level of security to your systems to ensure that someone accessing it has to provide a second form of identification (in addition to their password) to prove they are who they say they are.

NextWealth's Adviser Tech Stack report in 2020 illustrates the approaches taken by various adviser tech providers to security. At the time, two-factor authentication was rapidly becoming standard for back office systems and client portals. Most back office systems, cashflow modelling tools and client portals supported end client access. Back office systems and client portals almost universally allowed firms to upload client verification documents and other forms securely.

	Two-factor authentication		Username and password		Mix of approaches	Upload forms securely
	Adviser	Client	Adviser	Client		
Back office systems						
CURO (Time4Advice)	✓	✓				Yes
Intelligent Office (intelliflo)	✓		✓			Yes
True Potential	✓	✓	✓	✓		Yes
Turo	✓				✓	No
Xplan (Iress)	✓	✓				Yes
Cashflow modelling						
CashCalc	✓	✓	✓	✓		Yes
i4C	✓					No
Voyant	✓	✓				No
Suitability and risk profiling						
Defaqto Engage	Not provided		Not provided			No
Dynamic Planner			✓			Yes
FinaMetrica Toolkit (Morningstar)			✓			No
FinaMetrica Profilier (Morningstar)			✓			Yes
Client portal						
Advicefront	✓	✓			✓	Yes
Client Portal Xplan (Iress)	✓	✓				Yes
Client Portal Adviser Office (Iress)			✓	✓		Yes
Filehaven	✓	✓			✓	Yes
Moneyinfo	✓	✓			✓	Yes
The Personal Finance Portal (Intelliflo)	✓	✓	✓			Yes

"Multi-factor authentication is just the number one thing. We see an increasing number of our advisers and smaller third-party customers who have had their email compromised. In almost all the cases, they don't have multi-factor authentication and so their credentials are phished. They've got the email account, they're into the email account, and then they just use the email account to launch more phishing campaigns, or to send malicious content. But this is just that one simple thing you can do, enable multi-factor authentication and you are protecting against so much of that threat."

Adam Haylock, Global Head of Cyber Information and Security, Fidelity International

Use a password manager

Use a password manager at your firm that securely holds all of your various business account passwords and alerts you to any breaches.

Conclusion

It is very positive that more advice firms are seriously considering the risk posed to their businesses and clients by breaches of information security. All the signals point in one direction:

- A growing number and increasing sophistication of cyber attacks.
- The potential for more regulatory requirements in this area.
- An increasing awareness and demand from clients to ensure their data is well protected in our industry (whether by advisers or in its transference between adviser and provider and client).
- A growing reliance on technology at the heart of the financial advice proposition.

The great news is that addressing cyber security risk does not need to be overly complicated, and there are simple steps that businesses can take, some of them free of charge, to get an essential level of protection in place.

The key is that firms view cyber security as a core component of business risk and business planning, not as a special project, and that as such it is regularly revisited and kept front of mind for all staff in the firm.

Further reading

NCSC Cyber Essentials

Fidelity FundsNetwork's Keeping your business safe hub

10 steps to protect your business from a cyber attack

FundsNetwork

Fidelity INTERNATIONAL

UKM1121/37217/SSO/1122