



# Cyber threats to corporate pension schemes

# Table of contents

3	Introduction	15	Part 4: Third party providers
4	Executive summary	19	Part 5: Your critical assets
5	Profile of schemes	22	Part 6: Dealing with members
6	The Pensions Regulator expects	24	Part 7: Incident response
8	Part 1: Strategy, governance and documentation	27	Part 8: Financial impact
10	Part 2: Trustee risks	29	Next steps: Your cyber journey
13	Part 3: Scheme technology and processes	30	Appendix

# Introduction

The threats that cyber incidents pose to pension schemes have gone from unrecognised to unmissable in just a few years. As recently as five years ago the vast majority of pension schemes would not have had specific policies or processes to consider cyber threats. Fortunately, behind the scenes, most providers were generally alive to the risks and were managing them, even if they were not actively talking about them.

As the WannaCry ransomware swept through the NHS in May 2017, pension scheme trustees were starting to wake up to the issue. In April 2018 the Pensions Regulator issued its first guidance devoted to cyber risk, while in May 2018 GDPR introduced new controls around data. During 2019 the approach taken by pension scheme trustees continued to mature. Then as COVID-19 hit in 2020, schemes faced the twin challenges of increased cyber attacks (both on schemes and on members) and more of their scheme operations moving online.

It was in that environment that Aon launched the Pension Cyber Scorecard – a tool for UK trust-based pension schemes to assess their cyber resilience across a range of areas, and to see how they compare to other schemes. By the end of 2020 the Scorecard had been used by over 100 pension schemes, and this report summarises the responses to date.

It shows a mixed pattern across the industry, with some schemes having strong governance across all areas and some only just starting their cyber journey. The difference between the two is in some ways stark, but in other ways modest, with schemes able to take their cyber controls from novice to proficient in relatively short order.

In this report we highlight the results across those schemes, sharing previously unavailable data on the extent of cyber controls and governance that trustees have in place. We hope it is helpful, and that it gives schemes information that they can use to consider their own position, with the ultimate aim of protecting their scheme, their sponsor and their members.

To complete your own scorecard, visit [www.aon.com/cyberscorecard](http://www.aon.com/cyberscorecard).

For more information, contact us at [talktous@aon.com](mailto:talktous@aon.com)

**Paul McGlone**

Partner

Aon

February 2021

Introduction

Executive summary

Profile of schemes

The Pensions  
Regulator expects

Part 1: Strategy, governance  
and documentation

Part 2: Trustee risks

Part 3: Scheme technology  
and processes

Part 4: Third party providers

Part 5: Your critical assets

Part 6: Dealing with  
members

Part 7: Incident response

Part 8: Financial impact

Next steps:  
Your cyber journey

Appendix

# Executive summary

The assessments show a very mixed position, with some aspects of cyber security well managed across most schemes, while other aspects are still limited to just a minority of schemes.

- Strategically around **3 in 5** schemes have a cyber strategy.
- **75% of trustees have training on cyber risks.** Most schemes have some form of cyber-hygiene requirements, although details are very varied and fewer than **1 in 5 schemes have these documented clearly.**
- Trustee portals are now by far the most common way of sharing information (70%) and data (86%). However, **the majority of schemes undertake no checks on the security** of these portals, relying on the providers to do this on their behalf.
- Assessment of cyber controls at administrators is extensive, with almost **90% of schemes conducting checks.** For all other providers it is less than 50%.
- The nature of cyber checks is varied, with the most common approach being just to ask for the provider's standard documents. The **majority of schemes do no use specialist cyber expertise** to assess the responses.
- Understanding of the movement of scheme's data and assets is generally good, with data flows understood more clearly than flows of assets. Over 90% of schemes have a data breach policy, but **over one-third of schemes still send investment instructions in unencrypted emails.**
- Only **2 in 5 schemes have a robust incident response plan**, despite TPR guidance from April 2018 indicating that schemes should have one. **Over 60% of schemes believe they can rely on the sponsor's cyber security resources** in the event of an incident. In many cases this has not been tested.
- Over 60% of schemes have not assessed the potential financial impact of a cyber attack. Only **2% have a cyber insurance policy.**

The position is changing quickly within individual schemes and across the industry a whole. A scheme that is at the front of the pack this year could find themselves behind if they don't continue to develop their approach.

Introduction

▶ Executive summary

Profile of schemes

The Pensions  
Regulator expects

Part 1: Strategy, governance  
and documentation

Part 2: Trustee risks

Part 3: Scheme technology  
and processes

Part 4: Third party providers

Part 5: Your critical assets

Part 6: Dealing with  
members

Part 7: Incident response

Part 8: Financial impact

Next steps:  
Your cyber journey

Appendix

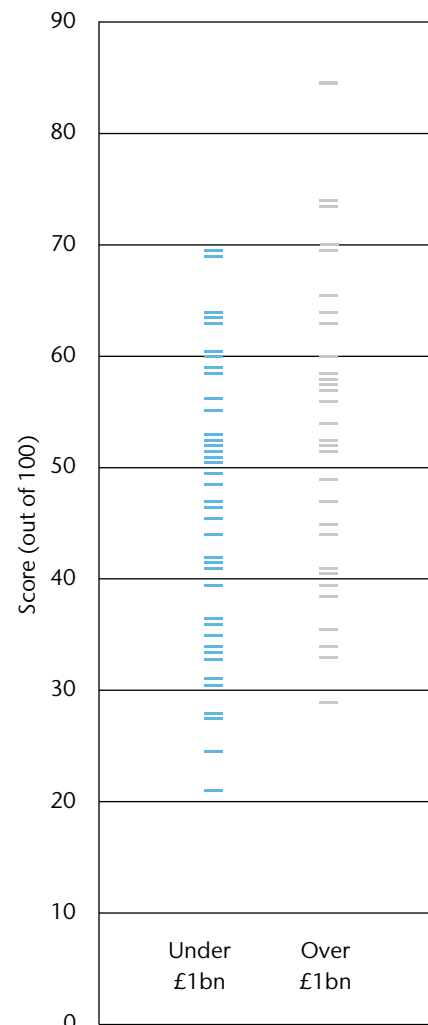
# Profile of schemes

The information analysed in this report was collected during the second half of 2020. Unlike a conventional survey, it was not all collected at one time, it was spread over about 6 months, as individual schemes decided to undertake their own assessment. The position of some schemes will have moved on since the assessment was completed, as it was a catalyst for improving their cyber resilience. But despite that, we are confident that the results remain representative of what is typical across UK trust-based pension schemes.

Overall the analysis covers 100 schemes, ranging in size from under £10m to over £10bn. The profile of these schemes included more representation of large schemes than the industry as a whole, with 40% having assets of more than £1bn. This reflects the fact that larger schemes have been faster to engage with this topic and complete the assessment. But surprisingly, the typical approach of larger and smaller schemes is not that different.

As well as considering individual questions, the scorecard generates a single score, out of 100, for every scheme that took part. As the chart opposite shows at the extremes there are some differences – the lower scoring schemes were small and the best scoring schemes were large— for the most part both larger schemes (defined here as over £1bn) and smaller schemes (under £1bn) typically scored between 35 and 65.

Our conclusion is that size is not a key determining factor of cyber resilience. Rather it is something which the market calls ‘cyber maturity’. Schemes that have identified and understood the issue and taken steps to address it come out well. Schemes that have not yet engaged with the issues do not. Fortunately, as we mention in the introduction and as we will show in this report, many of the gaps can be bridged relatively quickly.



Introduction

Executive summary

▶ Profile of schemes

The Pensions Regulator expects

Part 1: Strategy, governance and documentation

Part 2: Trustee risks

Part 3: Scheme technology and processes

Part 4: Third party providers

Part 5: Your critical assets

Part 6: Dealing with members

Part 7: Incident response

Part 8: Financial impact

Next steps: Your cyber journey

Appendix

## Seek | Shield | Solve

Cyber threats can be complex, and actions can initially be daunting, but a simple framework can help to focus actions. Aon's Seek Shield Solve framework is one such approach, which trustees can easily work with when putting their plans together.

### Overall cyber strategy



#### Seek

Understand and quantify the risk



#### Shield

Protect the Scheme and its critical assets



#### Solve

Be able to react and recover quickly

Throughout this document there are numerous practical steps that schemes can take, which fit naturally into one of the parts of this framework.

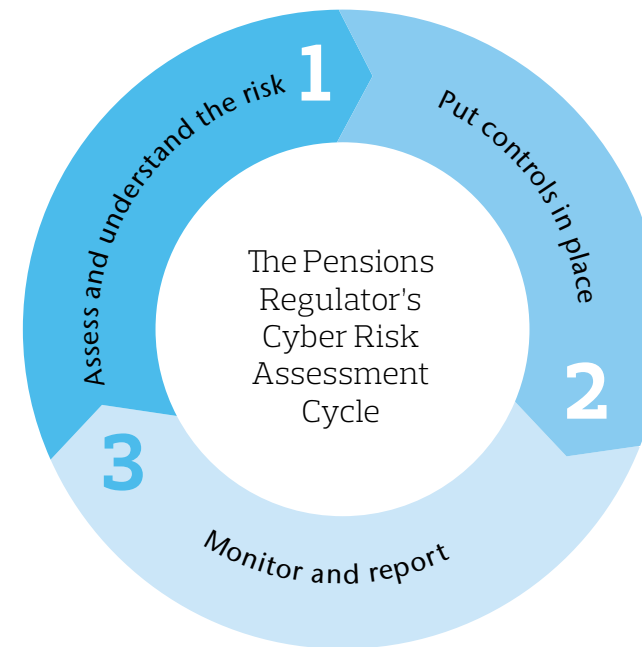
## The Pensions Regulator expects...

While some aspects of managing cyber risk are covered by legislation, they are relatively few. Under GDPR, schemes have certain obligations around data, but for the most part cyber controls are not explicitly required.

The closest that schemes have to specific requirements is the guidance issued by the Pensions Regulator in 2018, which outlines how the Regulator expects trustees to behave in relation to managing cyber risk.

In some senses the guidance is fairly basic, suggesting steps which are largely common sense. But basic doesn't mean widespread, and as the result of the scorecard analysis shows, almost three years on from its issuance, there are many schemes that have not yet formally considered these issues.

As well as providing a general backdrop for the assessments, the Regulator's guidance was cited as the acid test when answering questions. Schemes were asked only to respond 'yes' to questions about their actions if they were in a state in which they would be comfortable to share with the Regulator. Anecdotally, that had the desired effect, with many schemes telling us "strictly we do have that..." (for example, an incident response plan) "...but honestly it's not great and needs more work".



Introduction

Executive summary

Profile of schemes

▶ The Pensions Regulator expects

Part 1: Strategy, governance and documentation

Part 2: Trustee risks

Part 3: Scheme technology and processes

Part 4: Third party providers

Part 5: Your critical assets

Part 6: Dealing with members

Part 7: Incident response

Part 8: Financial impact

Next steps:  
Your cyber journey

Appendix



# Extract from the Pensions Regulator's “Cyber Security Principles for Pension Schemes”

April 2018

## Assess and understand the risk

- Do you understand the cyber risk facing your scheme:
  - your key functions, systems and assets
  - your cyber footprint, vulnerabilities and impacts?
- Is the cyber risk on your risk register and is it regularly reviewed?
- Do you have access to the right skills and expertise to understand and manage the risk?

## Put controls in place

- Are sufficient controls in place to minimise the risk of a cyber incident occurring:
  - IT security controls
  - processes
  - people?
- Have you assured yourselves of your third-party providers’ controls?
- What standards or accreditations help you or your suppliers demonstrate cyber readiness?
- Do you have a response plan in place to deal with any incidents which occur and help you swiftly and safely resume operations? Do your suppliers?
- Are you compliant with data protection legislation (including readiness for the General Data Protection Regulation)?

## Monitor and report

- Are your controls, processes and response plans regularly tested and reviewed?
- Are you clear on how and when incidents would be reported to you and others including regulators?
- Are you kept regularly updated on cyber risks, incidents and controls?
- Are you keeping up to date with information and guidance on threats?

Introduction

Executive summary

Profile of schemes

▶ The Pensions  
Regulator expects

Part 1: Strategy, governance  
and documentation

Part 2: Trustee risks

Part 3: Scheme technology  
and processes

Part 4: Third party providers

Part 5: Your critical assets

Part 6: Dealing with  
members

Part 7: Incident response

Part 8: Financial impact

Next steps:  
Your cyber journey

Appendix

# Part 1: Strategy, governance and documentation

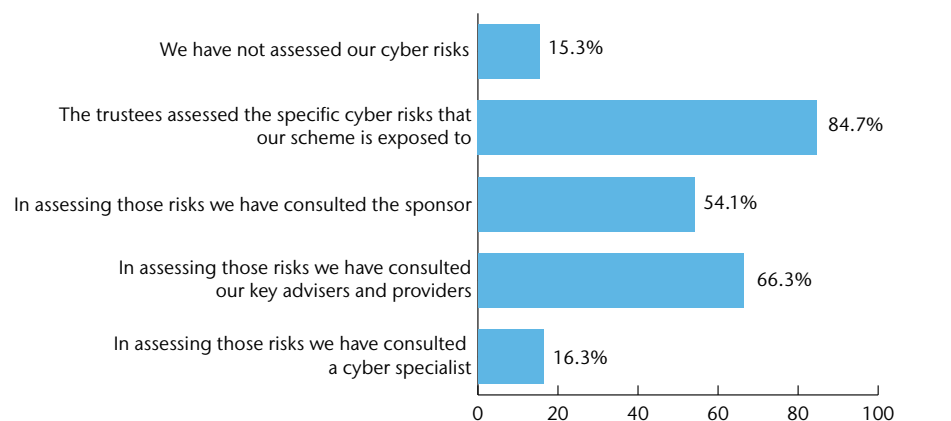
The starting point in managing any risk is to understand the nature of that risk. We therefore asked schemes whether they had taken active steps to assess their cyber risk.

The good news is that 85% of schemes said that they had. While fewer had consulted their sponsor, their advisers or a cyber specialist, this is still an encouraging start.

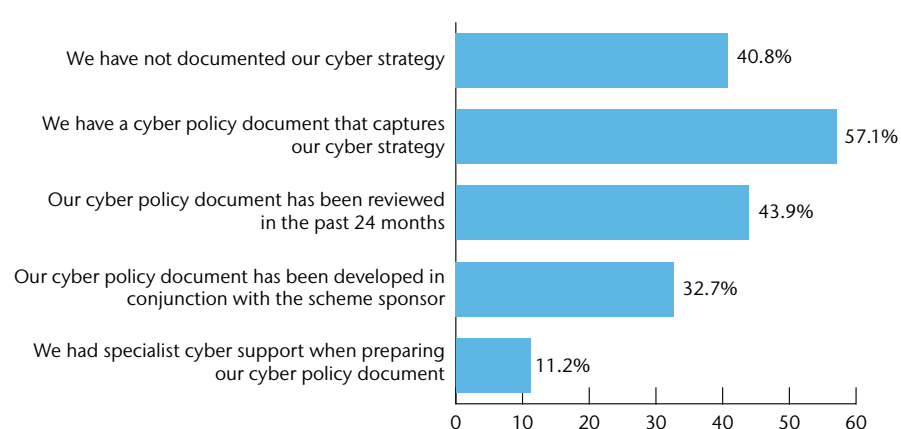
Perhaps more concerning is the anecdotal evidence from our discussions with schemes, which is that in many cases the assessment is almost exclusively focused on member data and GDPR. While data is a crucial part of cyber security it is not the only issue, as the case studies and actions in the remainder of this document will demonstrate.

Having understood the risks, our next question was whether schemes had an overall strategy to deal with those risks. While 57% of schemes said that they do, over 40% of schemes do not, even among many of the larger and more cyber-aware schemes. A cyber strategy in isolation does not, of course, reduce risk. But in our experience, it shines a light on the overall approach to cyber threats, and usually result in gaps being identified and filled.

## How have you assessed your cyber risks?



## How is your scheme's cyber strategy documented?



Introduction

Executive summary

Profile of schemes

The Pensions Regulator expects

▶ Part 1: Strategy, governance and documentation

Part 2: Trustee risks

Part 3: Scheme technology and processes

Part 4: Third party providers

Part 5: Your critical assets

Part 6: Dealing with members

Part 7: Incident response

Part 8: Financial impact

Next steps: Your cyber journey

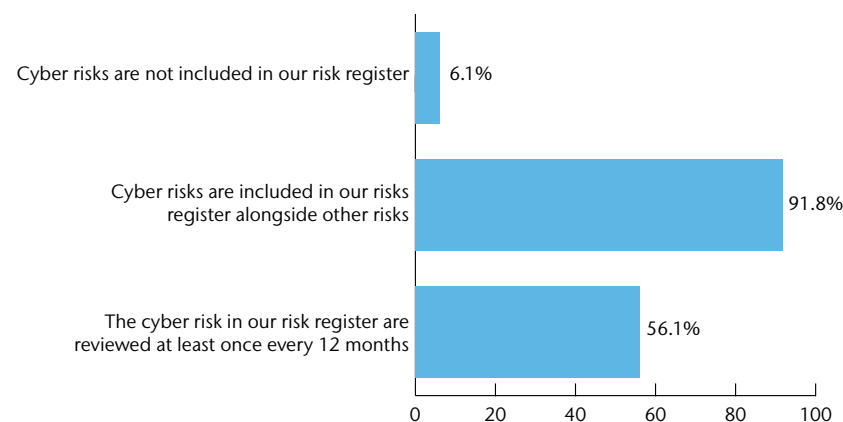
Appendix



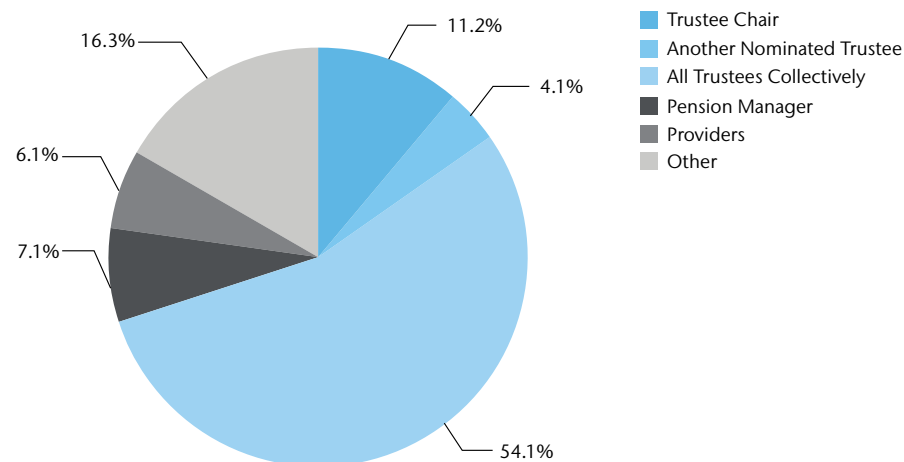
Related to this, we asked whether schemes included cyber risk on their risk register. Encouragingly, over 90% confirmed that they did. In the longer term, the risk register (and other areas such as internal controls) are the natural homes for cyber risks – sitting alongside a scheme’s other risks. In the short term, however, as an emerging and evolving risk, we believe that additional controls such as a cyber strategy are helpful.

Finally in this section, we asked who had primary responsibility within the scheme for cyber risk. Over half of schemes stated that all trustees collectively were responsible, and legally this is true – ultimately accountability is with all trustees and cannot be delegated. But responsibility to take actions forward can be delegated, and we find that in practice more specific ownership of cyber issues tends to result in actions being taken more quickly.

### How do your cyber risks link to your risk register?



### Who has primary responsibility for cyber risks?



## Part 2: Trustee risks

While the majority of a pension scheme operation is outsourced to third parties, trustees themselves have a role to play, not just in overseeing the providers they appoint but in ensuring that they themselves are not the weakest link.



### Case study: Compromised email and fake instructions

**A common scam that cyber criminals use is to pretend to be someone they are not. There are many variations of this type of scam, the sequence of events below is just one example:**

- Trustee Director, Mr T, had his email account compromised, but didn't realise.
- The hacker, H, spent time reviewing email history and contacts.
- H sent an email to the Finance Director, Ms F, advising that one of the scheme's major suppliers had changed their bank details. Attached to that was a fake email from the supplier (which H had also created) with the new details.
- Ms F emailed back to say an email was not sufficient and that a letter would be required. That email was intercepted by H, so never reached Mr T.
- H replied soon afterwards with a PDF of a letter from the provider, on their headed paper and signed by genuine contacts (all details available from Mr T's email account).
- Ms F approved the changes and paid a six-figure sum to the fake account.
- The issue was identified when Mr T and Ms F had a conversation and it became apparent that Ms F had acted on instructions that Mr T knew nothing about.

**What processes does your scheme have which would have avoided this issue?**

For many years schemes have had expectations of trustee behaviour. Common sense things such as not discussing individual cases with members or shredding confidential information after meetings. The 21<sup>st</sup> century equivalents are more digital in nature, and we asked schemes what types of 'cyber-hygiene' requirements they place on their trustee. The results were mixed, and in practice this is an area that is still evolving.

On the thorny topic of using home email addresses — something that is common among member-nominated trustees — around 40% of schemes now have a policy that trustees should not use a home email address that they use for other purposes. At the other extreme, we are now seeing some larger schemes considering whether to set up their own email domain.

Introduction

Executive summary

Profile of schemes

The Pensions  
Regulator expects

Part 1: Strategy, governance  
and documentation

▶ Part 2: Trustee risks

Part 3: Scheme technology  
and processes

Part 4: Third party providers

Part 5: Your critical assets

Part 6: Dealing with  
members

Part 7: Incident response

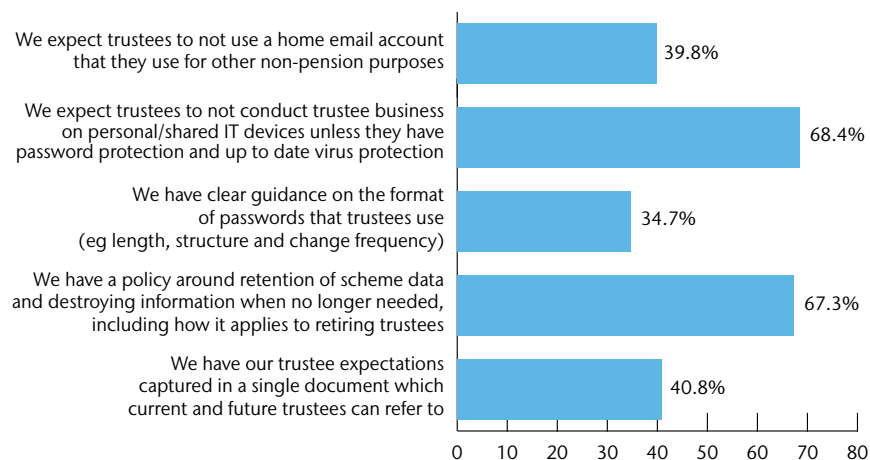
Part 8: Financial impact

Next steps:  
Your cyber journey

Appendix

- Introduction
- Executive summary
- Profile of schemes
- The Pensions Regulator expects
- Part 1: Strategy, governance and documentation
- ▶ Part 2: Trustee risks
- Part 3: Scheme technology and processes
- Part 4: Third party providers
- Part 5: Your critical assets
- Part 6: Dealing with members
- Part 7: Incident response
- Part 8: Financial impact
- Next steps: Your cyber journey
- Appendix

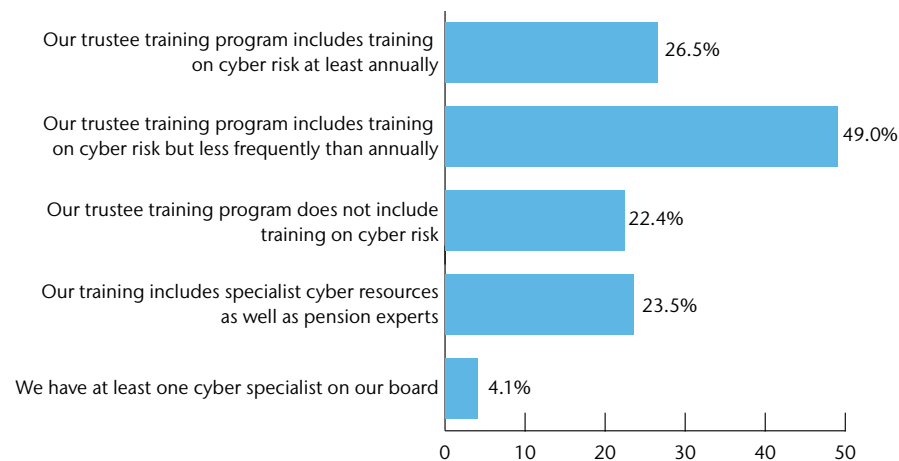
### What are your expectations of trustees?



Almost 90% of the schemes assessed had at least one of the above controls. But less than 20% had all the suggested controls.

Alongside specific controls, trustee training has a role to play in ensuring that trustees understand the risks and keep themselves and their scheme safe. Our data shows that around 75% of trustees now have some form of cyber training, although only 23% use cyber specialists to deliver that training. On the specific issue of phishing, which is an obvious threat to trustees, while many have had some training on identifying such emails through their day job, many trustees still have not.

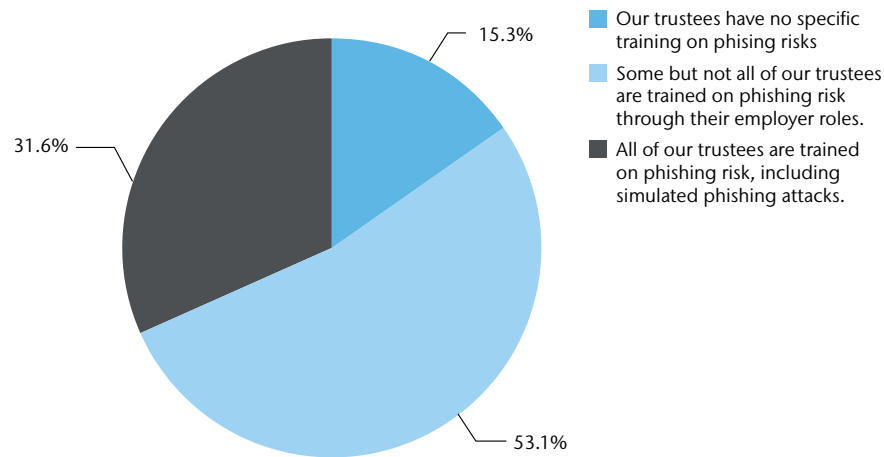
### Details of your trustee training and expertise





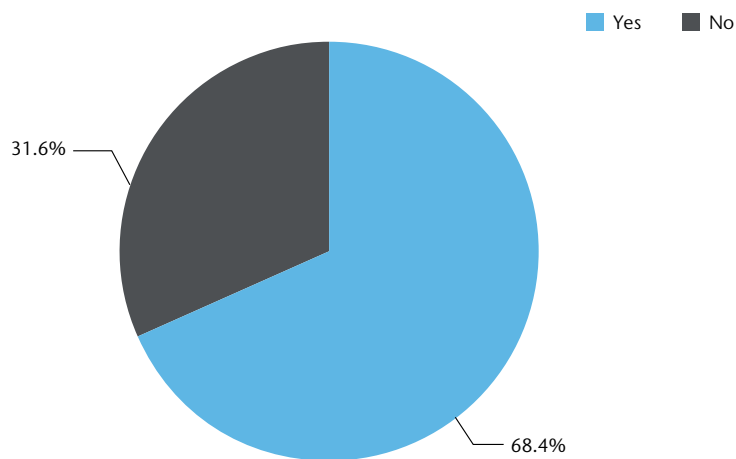
- Introduction
- Executive summary
- Profile of schemes
- The Pensions Regulator expects
- Part 1: Strategy, governance and documentation
- ▶ Part 2: Trustee risks
- Part 3: Scheme technology and processes
- Part 4: Third party providers
- Part 5: Your critical assets
- Part 6: Dealing with members
- Part 7: Incident response
- Part 8: Financial impact
- Next steps: Your cyber journey
- Appendix

### Have trustees received training on phishing risks?



Finally, around 70% of trustees now get periodic updates on cyber threats that face the scheme, although the question did not specify who these updates might come from.

### Do trustees receive periodic cyber updates?

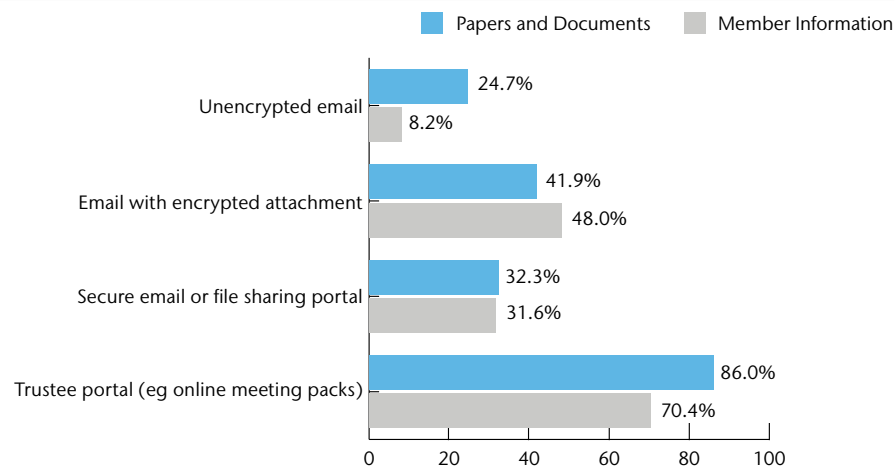


# Part 3: Scheme technology and processes

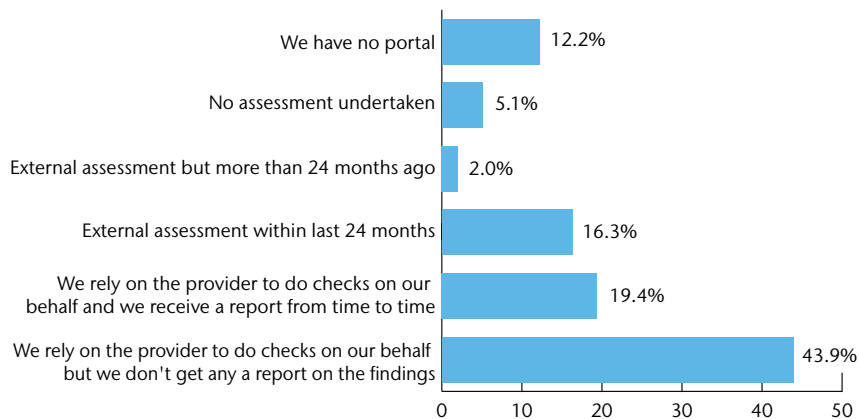
For the most part, pension schemes use third parties to process data and other aspects of the scheme. But certain items are done by the trustees alone, often through emails or portals. Across the schemes completing this assessment, secure trustee portals are now the most popular way to share confidential information, whether that is meeting papers or member information. But the practice is not yet universal and risks remain for some schemes where trustees are using personal email or even paper meeting packs to share sensitive scheme information.

When it comes to reliance on those portals, the risk appears to be that trustees may be complacent about the security that such portals offer. While a minority actively assess the security of the portal that they use, the vast majority just rely on the provider, often without any reporting back to them. Is this a risk? Our experience is that these portals are generally set up well, and certainly more secure than an unencrypted email. But without asking the question, a trustee board cannot really know.

**Which approaches are used to information between trustees?**



**When was the security of your portal last assessed?**





## Your confidential information

As cyber threats become more widely understood by trustees, so does the scope of what trustees consider confidential or at risk.

- **Member data** has always been recognised as something to be protected.
- Disinvestment instructions are increasingly a concern, with hackers targeting **scheme assets**. As SIPs were put online in October 2020, many schemes realised that publicly available trustee signatures could pose a risk.
- And schemes looking at **corporate information** are very aware that what they have could be price-sensitive and should not be distributed without strong security.

\*\*\*\*

## Guess the password

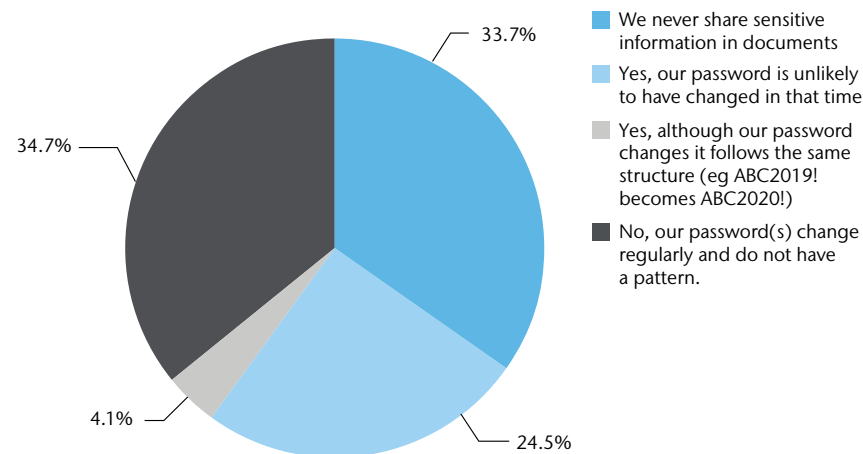
The ABC Pension Scheme has a password this year of ABCPS2021!

Last year it was ABCPS2020!

**What do you think it will be next year?**

Finally in this section, we asked about passwords that apply to trustee documents, inspired by the numerous schemes that we see using passwords that are easily guessed. The results concluded that, among those schemes that do share information in password-protected documents, just under half of those schemes have an approach that a former adviser or trustee could still guess over a year after leaving the scheme.

### Would a former trustee still be able to access password-protected documents?



## Part 4: Third party providers

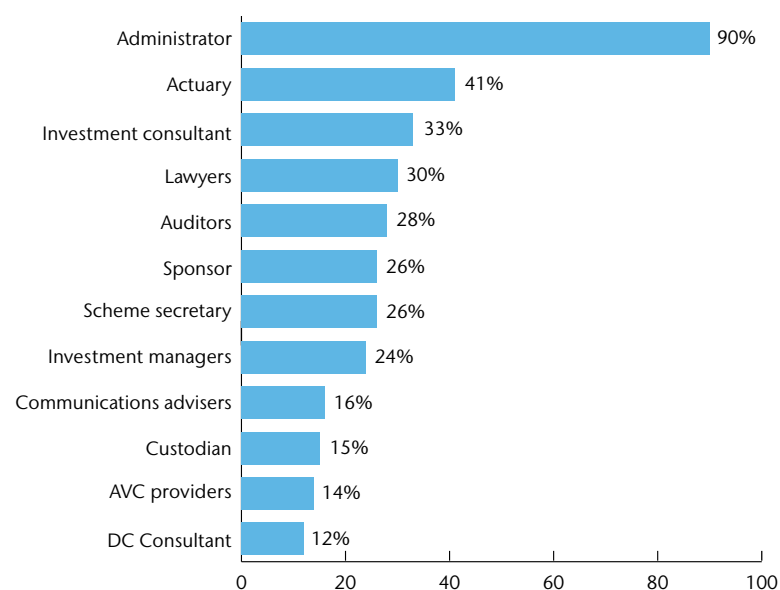
Assessing third party providers is perhaps the most easily understood activity that we see, and amongst the most common. Pension schemes outsource almost all material activities to third parties, whether that is administrative tasks (member administration, payroll, communication, preparation of account) or advice (legal, actuarial, investment etc).

Those providers therefore represent the front line of cyber defense and a number of industry bodies have recognised this in the guidance that they have issued, including the Pensions Regulator ('Cyber security principles for pension schemes, April 2018), the Pensions Administration Standards Association ('Cybercrime Guidance', November 2020) and the Pensions Research Accountants Group ('Cyber protection guidance' October 2020)

Looking at which providers are assessed, the administrator is by far the most common, with over 90% of schemes having done some sort of assessment.

Across the schemes responding to this assessment, over 80% relied on third party administrators, with a minority using in-house teams. Although there were no stark differences in how these schemes had assessed their administrators, in practice we see a difference in how that process works, with many schemes finding that their sponsor's IT team is vouching for the security of their own organisation's systems. As a contrast, in areas such as covenant assessment, trustees are expected to seek an independent opinion rather than just accept the word of the sponsor. We see this same philosophy now making its way into cyber assessments.

Which providers have you assessed in the past 24 months?



Introduction

Executive summary

Profile of schemes

The Pensions Regulator expects

Part 1: Strategy, governance and documentation

Part 2: Trustee risks

Part 3: Scheme technology and processes

▶ Part 4: Third party providers

Part 5: Your critical assets

Part 6: Dealing with members

Part 7: Incident response

Part 8: Financial impact

Next steps: Your cyber journey

Appendix

Looking across other providers, the prevalence of cyber assessments is less common. Again, that is as we would expect, although we expect these numbers to increase. It is undoubtedly the case that not all providers are equal, and as schemes settle on a periodic review of advisers we find advisers being grouped into tiers, with the higher risk providers being reviewed more frequently than lower risk providers. For providers that are lowest on this list (notably DC and AVCs), this is in part due to some schemes not having such providers. However, of those schemes that told us that they had a DC section to their scheme, only 25% of those schemes advised that they had reviewed the cyber controls of their DC provider.

## Case study: Sponsor impact on scheme

For one unfortunate in-house pensions team, a cyber-attack on the sponsor created significant disruption not just to the staff and customers, but also to pension scheme members.

This scheme hadn't thought about what would happen if a cyber attack occurred and the sponsor also hadn't considered the pensions team's needs in significant detail when they established their incident response plan. So when the company was paralysed by malware, response efforts focused on restoring the business operation but it took several weeks to get email back up and running, and a lot longer to restore the pensions teams files; as this hadn't been considered high priority in the recovery efforts.

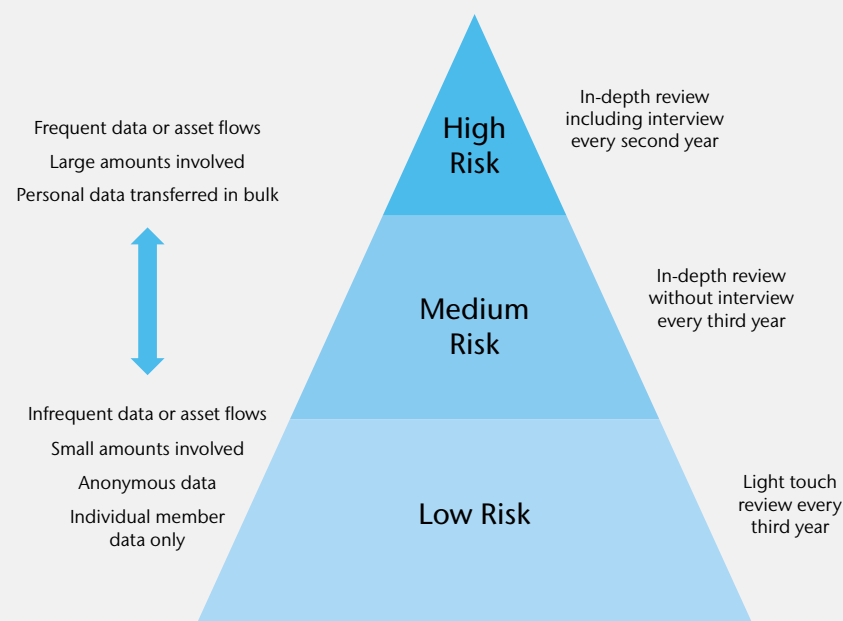
This slow recovery created bottle necks with processing member requests, challenges with authorising payments, and frustration for members calling up seeking assistance.

Following the attack contingency plans have been developed, company incident response plans improved and a pension scheme plan created.

## What makes a provider high risk?

Allocating providers into tiers based on risk levels is a practical way to manage your cyber budget, with high risk providers being reviewed more frequently, and in more detail, than low risk providers. Depending on the nature of the provider, that can be assessed based on the membership data that they work with, the assets or transactions that they touch, or the confidential information that they hold. Asset and data mapping can help with this, as shown on page 20.

### Possible tiered cyber review framework



Introduction

Executive summary

Profile of schemes

The Pensions  
Regulator expects

Part 1: Strategy, governance  
and documentation

Part 2: Trustee risks

Part 3: Scheme technology  
and processes

▶ Part 4: Third party providers

Part 5: Your critical assets

Part 6: Dealing with  
members

Part 7: Incident response

Part 8: Financial impact

Next steps:  
Your cyber journey

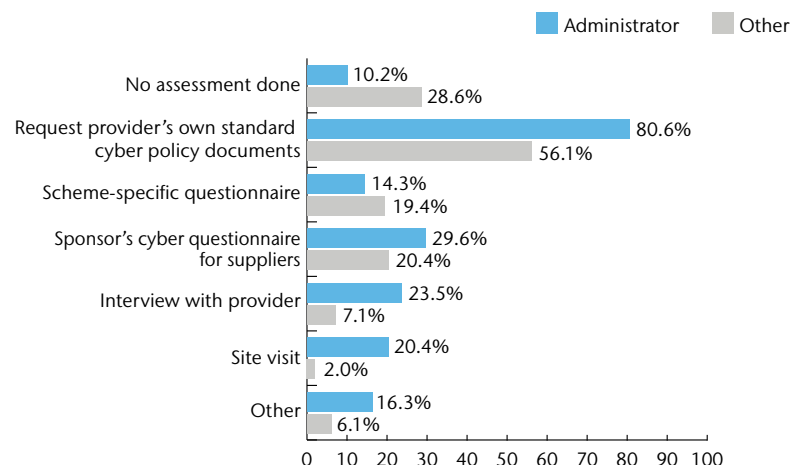
Appendix



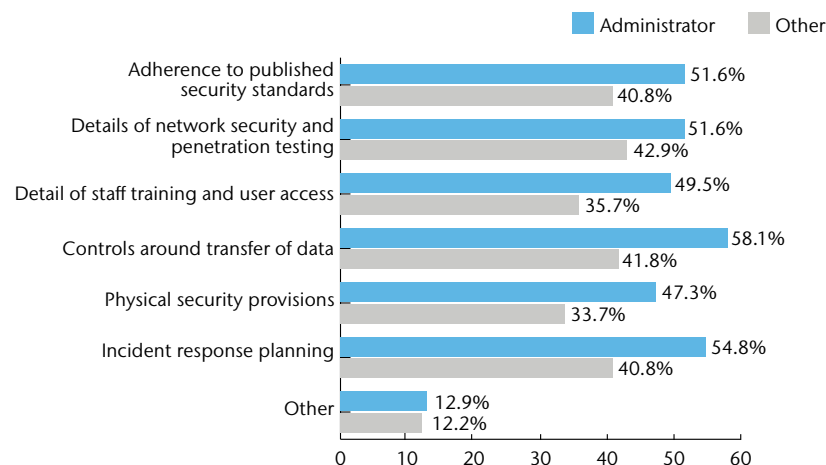
- Introduction
- Executive summary
- Profile of schemes
- The Pensions Regulator expects
- Part 1: Strategy, governance and documentation
- Part 2: Trustee risks
- Part 3: Scheme technology and processes
- Part 4: Third party providers
- Part 5: Your critical assets
- Part 6: Dealing with members
- Part 7: Incident response
- Part 8: Financial impact
- Next steps: Your cyber journey
- Appendix

We also asked schemes about the nature of their assessments: who they were conducted by, how they were conducted, and what areas they covered. The results are very mixed, and are shown in the charts below.

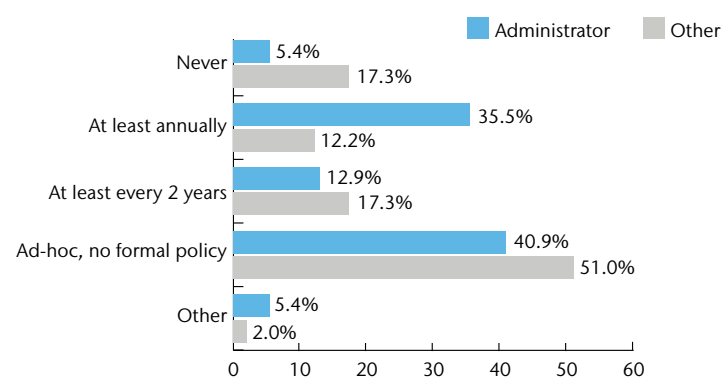
### How do you assess providers?



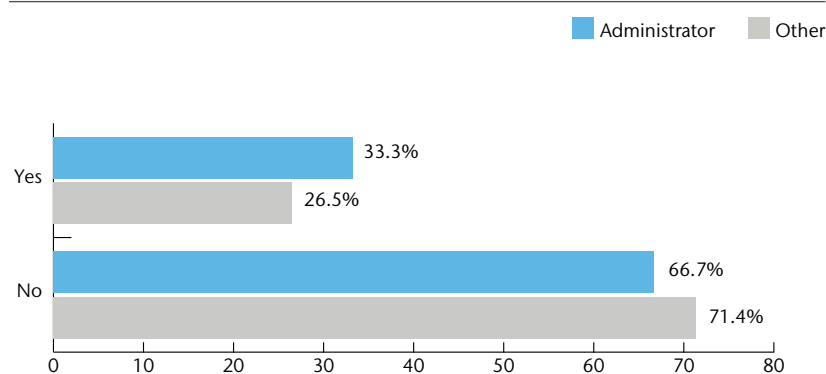
### Which of these areas did your last assessment cover?



### How often do you typically assess providers?



### Did you use specialist cyber expertise?



This range of responses has to be expected in an industry where cyber-assessment of providers is an emerging issue that many schemes are doing for the first time. But a couple of themes emerge from the results and from our day-to-day dealings with schemes:

- **The support of a sponsor can be a great help**

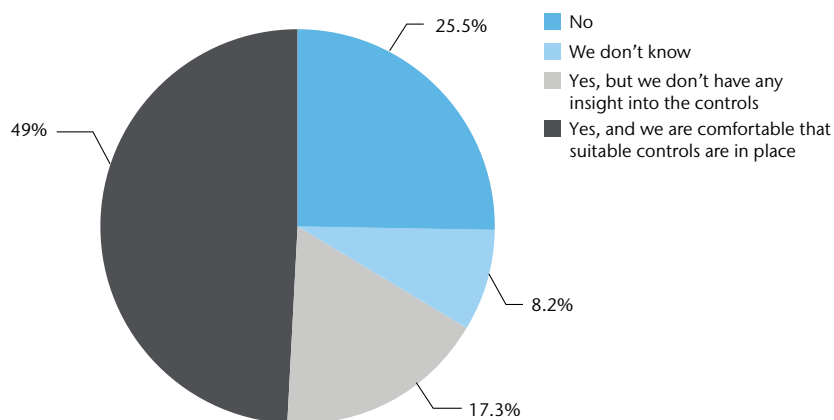
Pension schemes tend to not have IT and cyber expertise available, but many sponsors do, and routinely use that expertise to vet their own providers. If a scheme can use the same process, then that can be a good outcome.

- **Understanding the responses is hard**

Asking questions of providers is the easy part. Understanding the responses is harder, and trustees can find themselves none the wiser unless they have someone they can rely on to interpret the responses and to help them understand whether they are adequate.


We also asked schemes how they deal with sub-contractors. Only about 8% of schemes did not know whether sub-contractors were used, while the majority confirmed that they were comfortable with the controls that existed.

### Does your data ever get shared with subcontractors?



Before moving on it is worth stressing that nothing in this assessment is about whether pension scheme providers and advisers are secure — it is about whether trustees have asked the question. In our experience, all the major pension firms take security very seriously, and in assessments in which our clients have been involved, almost all providers have been able and happy to demonstrate their credentials.

However, trustees cannot rest on their laurels and assume that will remain the case. As with any industry, no pension provider would claim to be invulnerable. As technology and services evolve, so do the risks and the mitigations required.



## Industry standards

While this section has focused on assessments that trustees might conduct themselves, schemes should be aware that various industry standards exist which they can usefully refer to.

Industry cyber frameworks such as those issued by NIST (National Institute of Standards and Technology) and the NCSC (National Cyber Security Centre) are often referred to when considering cyber risk. ISO27001 is an international standard on the management of information security, which many pensions providers align with if not formally certified. All have similarities but also different focuses.

Administrators will often have annual reports on how they comply with AAF 01/06, which includes cyber controls alongside other measures. And increasingly UK businesses are signing up to Cyber Essentials or Cyber Essentials plus, both operated by the National Cyber Security Centre.

Depending on the level of detail that schemes want to go into, these can be useful external standards to consider. But if schemes are going to rely on them, then they should understand what they cover and what they do not.

- Introduction
- Executive summary
- Profile of schemes
- The Pensions Regulator expects
- Part 1: Strategy, governance and documentation
- Part 2: Trustee risks
- Part 3: Scheme technology and processes
- ▶ Part 4: Third party providers
- Part 5: Your critical assets
- Part 6: Dealing with members
- Part 7: Incident response
- Part 8: Financial impact
- Next steps: Your cyber journey
- Appendix

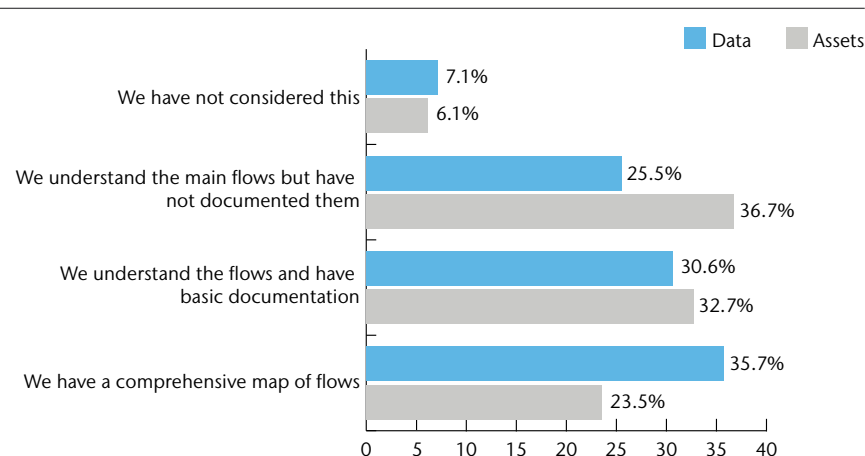
# Part 5: Your critical assets

A question often used by cyber specialists when assessing an organisation is ‘what are your critical assets’? For a pension scheme the most common answers are “our member data and our assets”. Therefore, understanding those assets is key to understanding your cyber threats.

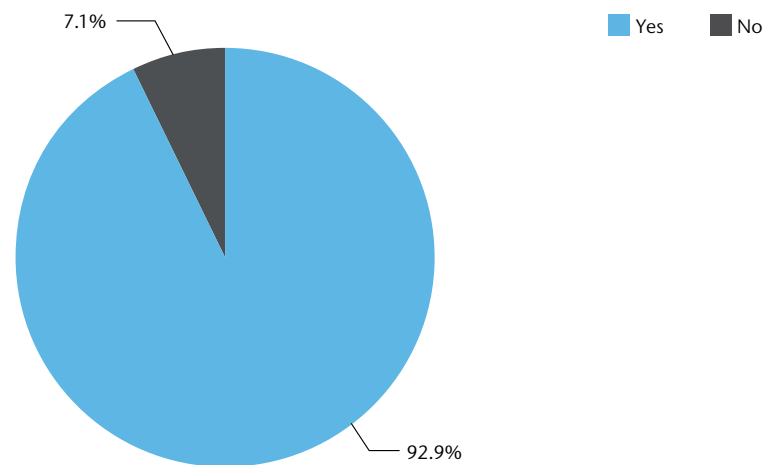
When asked how well they understand the flow of data and assets, around 65% of schemes advised that they had a data map, and 55% have an asset map. However, only 35% and 23% were prepared to say that what they had was comprehensive.

For data in particular, many schemes have data maps that originate from work done as part of GDPR compliance. With over 95% of schemes telling us that they have a data breach policy, GDPR compliance is clearly taken seriously. But since 2018 we have seen data and asset maps go beyond those initial attempts, with greater granularity, and with the intention that they are not only there for compliance purposes but as an active tool to help manage risk.

## Describe your understand of data and asset flows



## Do you have a data breach policy?



- Introduction
- Executive summary
- Profile of schemes
- The Pensions Regulator expects
- Part 1: Strategy, governance and documentation
- Part 2: Trustee risks
- Part 3: Scheme technology and processes
- Part 4: Third party providers
- Part 5: Your critical assets
- Part 6: Dealing with members
- Part 7: Incident response
- Part 8: Financial impact
- Next steps: Your cyber journey
- Appendix

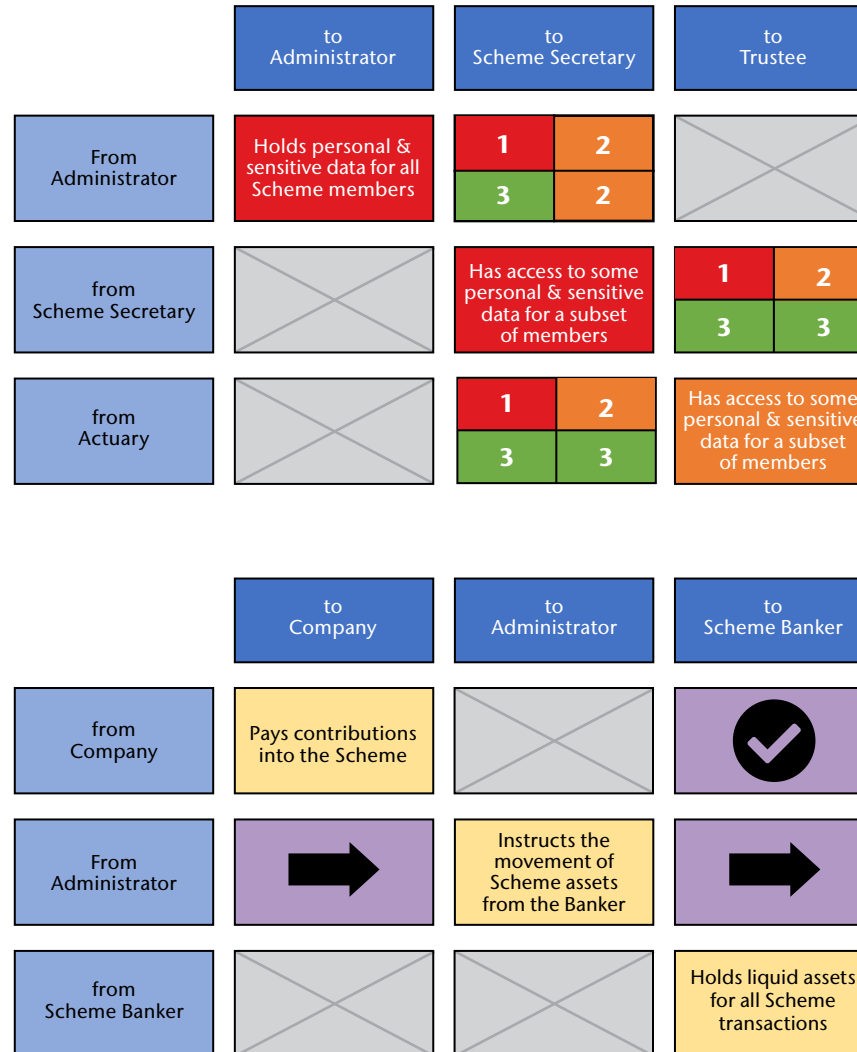
# A more granular map

A typical data or asset map is a spider's web of boxes and arrows, showing how information flows around the system. But not all boxes and arrows are equal. How do you distinguish between the occasional flow of anonymous data through a secure portal and the regular issuing of personal sensitive data in an unsecured spreadsheet?

Second generation data and asset maps address these issues by looking not just at the existence of a flow of information, but the nature of that flow. Is it individual or bulk data? Is it personal sensitive data or anonymised? Is it a large asset transfer or a small one? Is it a transfer of money or a transfer of instructions? And so on.

By building this picture of the scheme's critical assets, schemes can prioritise where their time is spent.

## Extracts from a data map and asset map



We asked schemes what they knew about the channels used to deal with member data and assets. The results are summarised on the following page.

Introduction

Executive summary

Profile of schemes

The Pensions Regulator expects

Part 1: Strategy, governance and documentation

Part 2: Trustee risks

Part 3: Scheme technology and processes

Part 4: Third party providers

▶ Part 5: Your critical assets

Part 6: Dealing with members

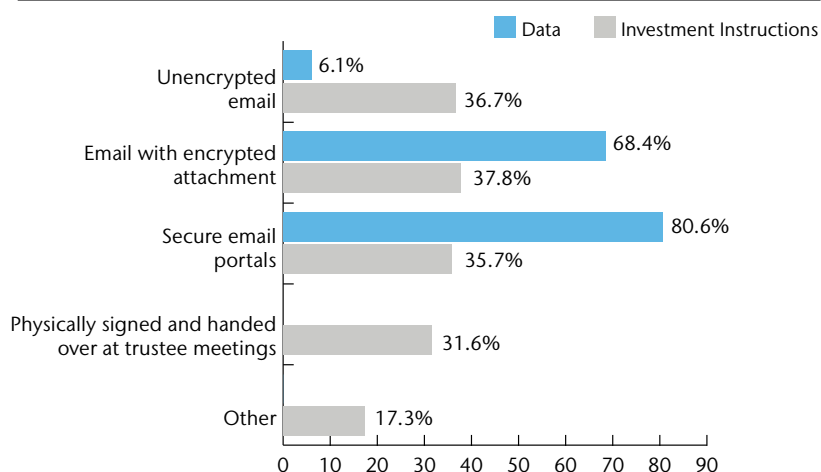
Part 7: Incident response

Part 8: Financial impact

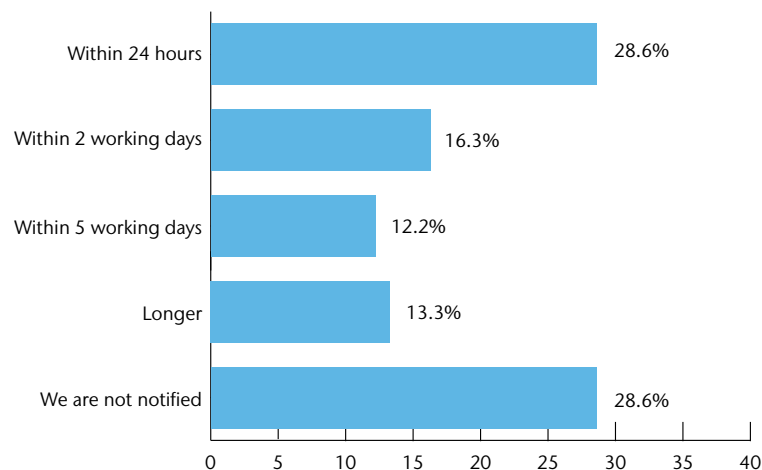
Next steps: Your cyber journey

Appendix

### How are member data and investment instructions circulated?



### How soon after an asset transaction are you notified?



As with exchanges between trustees, secure portals are now by far the most common way of sharing member data, although not universal. For asset transfers, the use of unencrypted emails was concerning and compounded by the fact that almost 30% of schemes are not notified as a matter of routine once a transaction has taken place.

That lack of reporting limits the opportunity to spot a fraudulent transaction should one occur, and is a concern. Of course, for schemes with fiduciary managers in place the arrangements the roles and responsibilities are different, with managers making decisions rather than trustees. Nevertheless, the same principles apply and although the process is different the question of ‘how long before someone would know?’ is equally valid.



## Case study: Fake investment instructions

In late 2020 new requirements came into force where schemes had to make their Statement of Investment Principles available on a publicly accessible website. Some schemes did so without thinking of the possible implications.

Within days of that deadline advisers and investment managers were aware of numerous cases of fake disinvestment instructions being identified. The obvious conclusion was that signatures had been extracted from those documents and that cyber criminals had been ready to collect and use them as they became available.

To the best of our knowledge all of these managers had safeguards in place which identified these attempts, and no money was lost. Most schemes have now removed signatures from their online statements, and have started to consider where else may contain publicly available trustee signatures.

Introduction

Executive summary

Profile of schemes

The Pensions  
Regulator expects

Part 1: Strategy, governance  
and documentation

Part 2: Trustee risks

Part 3: Scheme technology  
and processes

Part 4: Third party providers

▶ Part 5: Your critical assets

Part 6: Dealing with  
members

Part 7: Incident response

Part 8: Financial impact

Next steps:  
Your cyber journey

Appendix

# Part 6: Dealing with members

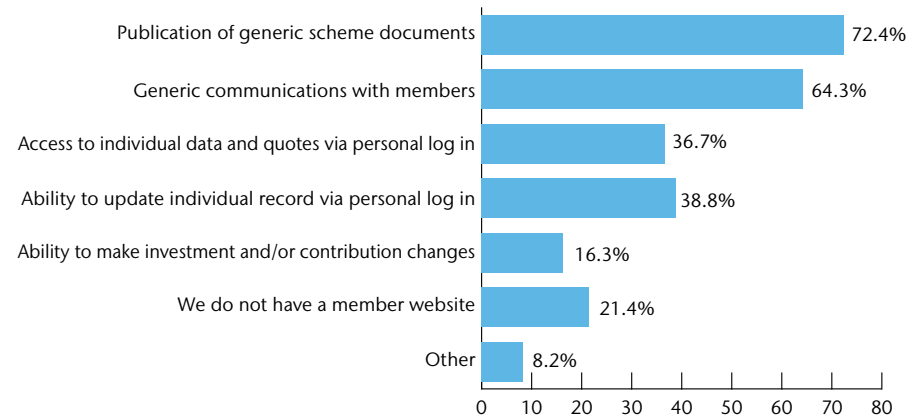
Ultimately any pension scheme exists for the benefits of its members, and the cyber threat works in both directions. A cyber attack on a scheme or its providers can impact on members, but equally an attack on a member could impact on the scheme. Understanding interactions with members is therefore yet another aspect of managing your cyber resilience.

We started by asking schemes about interactions with members through a website or app. The majority of schemes who responded indicated that they had some sort of web access for members but less than 40% indicated that members had access to personal information. This figure is undoubtedly higher than the market as a whole, and reflects the fact that the assessments have an over-representation of large schemes.

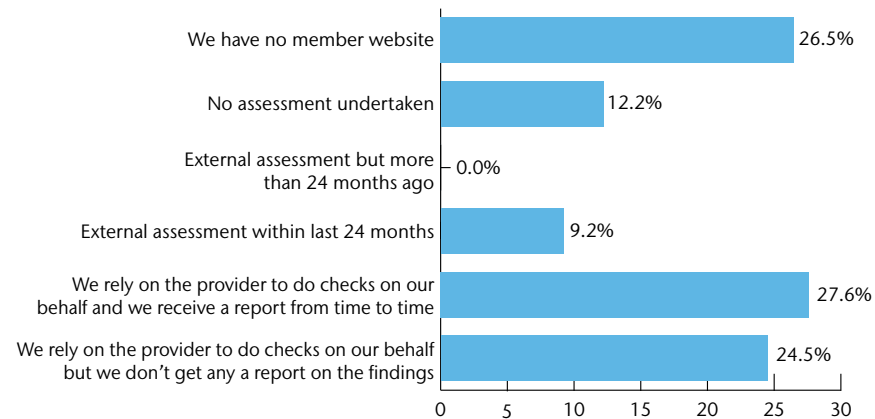
We fully support schemes who want to provide this functionality to their members. Indeed with the advent of the pensions dashboard that sort of access will become almost universal. But with access comes risks, and schemes who want to offer that sort of technology need to manage the risks associated with it.

Where schemes do have a website, we asked what security checks are done. Of schemes with sites, only 13% had undertaken any external assessment, with the most common approach being for schemes to rely on the provider and without any sort of reporting on the checks undertaken.

## What is on your website/app?



## When was the security of your member website last assessed?



Introduction

Executive summary

Profile of schemes

The Pensions Regulator expects

Part 1: Strategy, governance and documentation

Part 2: Trustee risks

Part 3: Scheme technology and processes

Part 4: Third party providers

Part 5: Your critical assets

Part 6: Dealing with members

Part 7: Incident response

Part 8: Financial impact

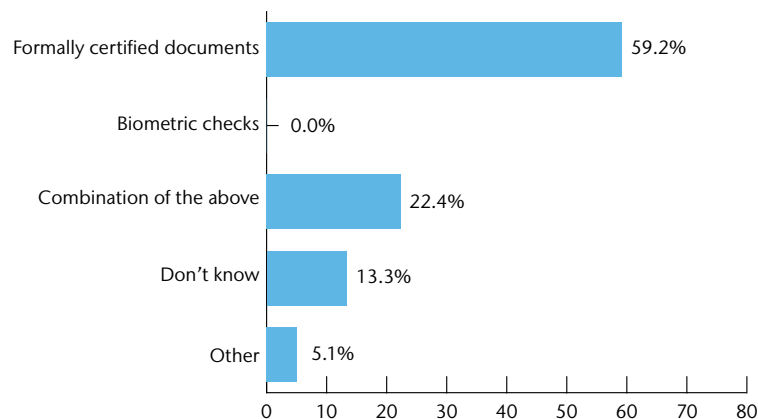
Next steps: Your cyber journey

Appendix

On the issue of verifying member identity, schemes and administrators have been doing this for many years and have tried and tested approaches. Most of them use a combination of personal data items to verify identity, and even if those completing the assessment did not know, those checks universally take place.

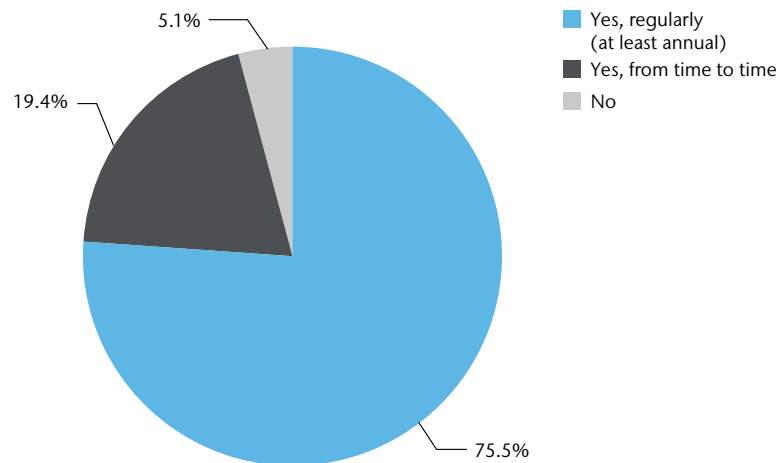
Over 20% of schemes completing the assessment now use a combination of digital methods and formally certified documents when putting benefits into payment. In practice the range of additional checks is quite varied, but various tools are now available to pension schemes to run checks that go beyond the traditional certified documents. With transfers and tax-free cash sums often amounting to many hundreds of thousands of pounds, we expect it is only a matter of time before such options are widely adopted by pension schemes to combat cyber security and member scams.

### What security arrangements are in place on your website/app?

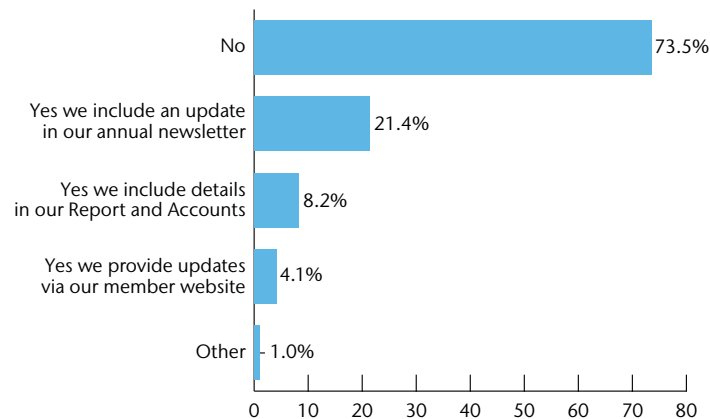


Finally, we asked schemes whether member communication covers cyber threats and the scheme's approach to cyber risk. While the vast majority (around 95%) warned members about the risk of scams and cyber threats, only around 1 in 4 informed members of the scheme's cyber policies.

### Are members warned of the risks of scams and cyber threats?



### Are members notified of scheme cyber security policies?



Of course, explaining the scheme's cyber policies does not in itself reduce risk. But it can be reassuring to members. As we say with the DC chair's statement, the requirement to explain to members how the scheme dealt with certain tasks was a catalyst for a rapid improvement in many areas. If as a trustee you cannot – or would be embarrassed to – explain your approach to a member, maybe that approach needs a review.

- Introduction
- Executive summary
- Profile of schemes
- The Pensions Regulator expects
- Part 1: Strategy, governance and documentation
- Part 2: Trustee risks
- Part 3: Scheme technology and processes
- Part 4: Third party providers
- Part 5: Your critical assets
- ▶ Part 6: Dealing with members
- Part 7: Incident response
- Part 8: Financial impact
- Next steps: Your cyber journey
- Appendix

## Part 7: Incident response

No matter how much the scheme and providers aim to prevent cyber attacks from being successful, nobody can be fully secure, and any organisation or individual could be on the receiving end of an attack. Schemes therefore need to be prepared.

Back in April 2018, the Pensions Regulator stated that “There should be an incident response plan in place to deal with incidents and enable the scheme to swiftly and safely resume operations”. In practice, while many schemes have aspects of a plan in place — 75% have a list of contacts available — only 40% have something that they would describe as a robust plan.

### Which components of an incident response plan do you have?



## Do you need a plan?

A comment that we often hear from trustees is that they don't need an Incident Response Plan. Instead they intend to rely on the provider's plan or that of their sponsor.

While those plans have a role to play, it is inevitably the case that the needs and priorities of the trustees may differ from those of the provider. For certain breaches the trustees may find that neither providers or employers are involved.

**A plan does not need to be comprehensive. But it's better than having no plan at all.**

Introduction

Executive summary

Profile of schemes

The Pensions Regulator expects

Part 1: Strategy, governance and documentation

Part 2: Trustee risks

Part 3: Scheme technology and processes

Part 4: Third party providers

Part 5: Your critical assets

Part 6: Dealing with members

▶ Part 7: Incident response

Part 8: Financial impact

Next steps: Your cyber journey

Appendix



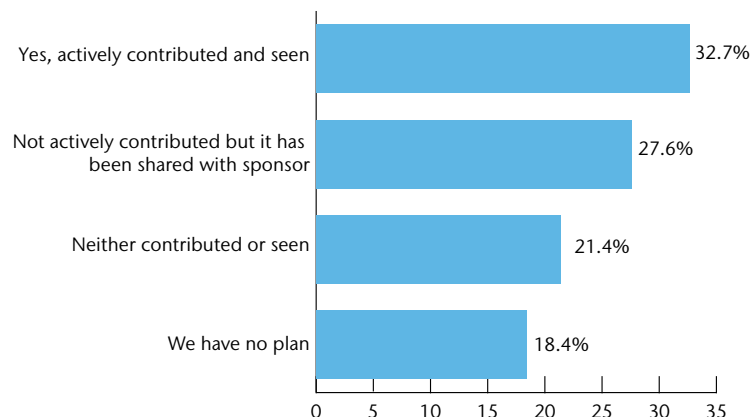
In an earlier section we looked at the extent to which schemes could rely on sponsor support when assessing third party providers. In this section we asked about support in the event of an incident.

Over 60% of schemes stated that they would have access to support from the sponsor’s cyber team in the event of an incident. We would be delighted if this were true, but have concerns over the reliability of such support. When asked whether the sponsor had contributed to the plan, only 30% of schemes said that they had. Is it realistic to expect that a sponsor will support a plan that they have had no part in developing? Anecdotally, for every scheme that we see supported by the sponsor, we see just as many where the trustees assume they have support, only to find that they when it comes to the crunch they don’t.

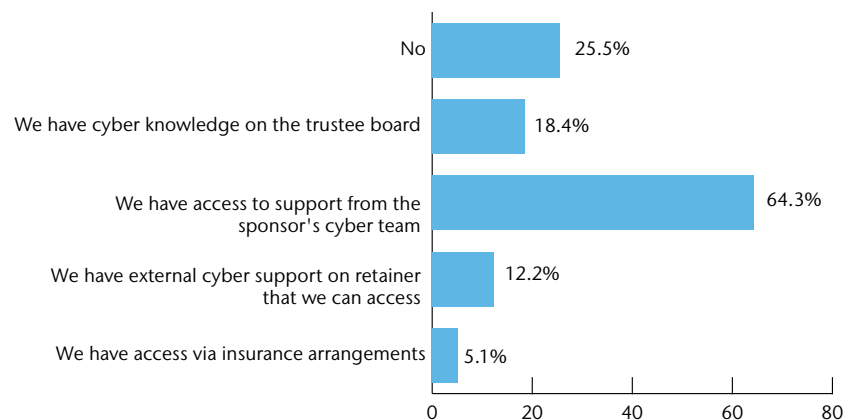
There are, of course other options. External support can be arranged, this is best done in advance, as some form of retainer, rather than rushing around in the middle of a crisis looking for support.

If a scheme can genuinely rely on the sponsor for support, this is often the best outcome all round. If you are a sponsor reading this report and you have not yet engaged with your pension scheme trustees on cyber risk, now may be a good time to do so.

### Have your incident response plans been seen and contributed by the sponsor?

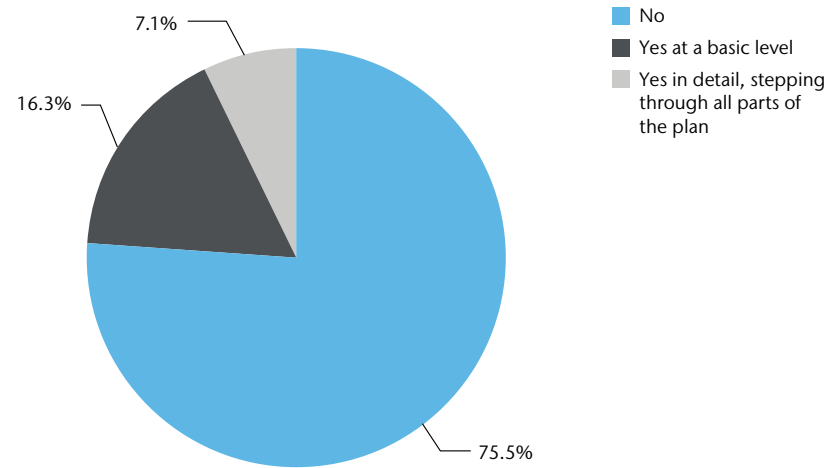


### Do you have access to specialist cyber support?

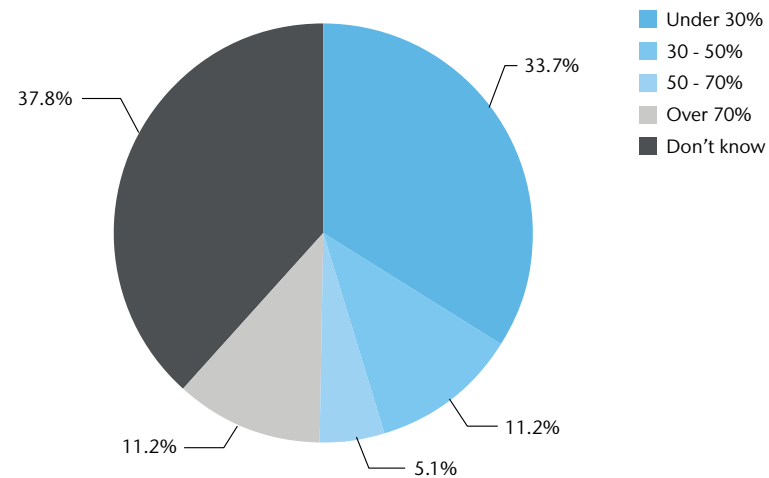


When we asked whether schemes had tested their plans, only 25% had done so. In our experience such tests are invaluable and result in substantial improvements. One specific item we asked schemes about was what proportion of members they could contact quickly by email if they needed to. While almost 40% did not know, the most common response was “under 30%”, suggesting that if an incident did occur, rapid member communication could be a serious challenge.

### Has your response to an incident been tested?



### What proportion of your members can you contact by email?



Introduction

Executive summary

Profile of schemes

The Pensions Regulator expects

Part 1: Strategy, governance and documentation

Part 2: Trustee risks

Part 3: Scheme technology and processes

Part 4: Third party providers

Part 5: Your critical assets

Part 6: Dealing with members

▶ Part 7: Incident response

Part 8: Financial impact

Next steps:  
Your cyber journey

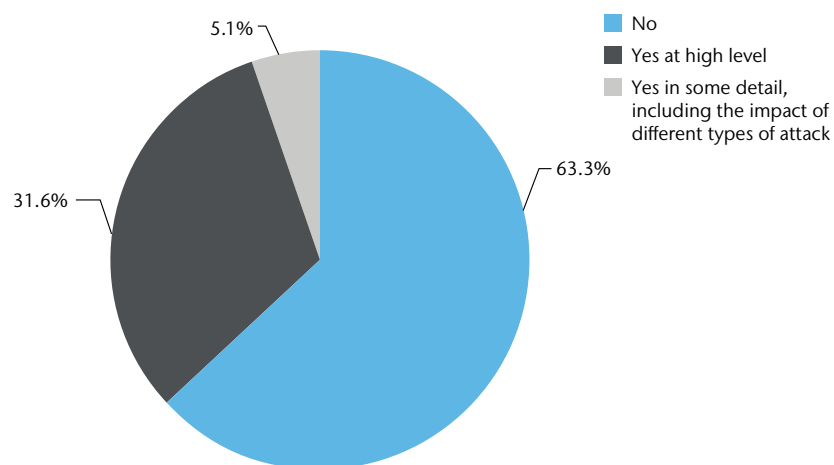
Appendix

# Part 8: Financial impact

The final set of questions we asked related to the financial impact of a cyber attack – something that we know is incredibly difficult to pin down.

As expected, most schemes (over 60%) have not done any sort of assessment, and only 5% have done an assessment in any detail. Given the range of possible attacks, from ransomware demands, to data theft to fake disinvestments, even a detailed assessment can only ever be a guess.

## Have you assessed the possible financial impact of a cyber attack?



For corporates a cyber assessment is not just an interesting exercise, it is also key to the next question which relates to cyber insurance. The first question that any insurer will ask is regarding what losses you require insurance for, and the potential size of those losses.

Cyber insurance is a growing market, but in the UK it is still only put in place by a minority of companies and almost no pension schemes. We asked what type of cover schemes had, looking at three possible types of policy:

- Over 45% of schemes told us that they were covered on their trustee indemnity policy. That is probably true, but such policies normally cover claims against the trustees. If a claim against the trustees arises because of a cyber incident impacting a 3<sup>RD</sup> party then it is probably covered. But if a cyber incident occurs without a claim then it probably isn't.
- Around 20% of schemes told us that they were covered on their employer's policy. We would be delighted if this were the case, but our experience makes us nervous. Depending on which data you look at, perhaps only 10-30% of employers have cyber insurance in the first place. Based on the policies that we have seen pension schemes and trustees are not normally named as a policyholder.
- Only 2% of schemes told us that they had their own policy. Pension-specific policies are certainly available and are not expensive. But they are uncommon, reflecting the fact that most cyber insurers do not understand pension schemes and most schemes cannot articulate and quantify their cyber exposures.

Introduction

Executive summary

Profile of schemes

The Pensions Regulator expects

Part 1: Strategy, governance and documentation

Part 2: Trustee risks

Part 3: Scheme technology and processes

Part 4: Third party providers

Part 5: Your critical assets

Part 6: Dealing with members

Part 7: Incident response

▶ Part 8: Financial impact

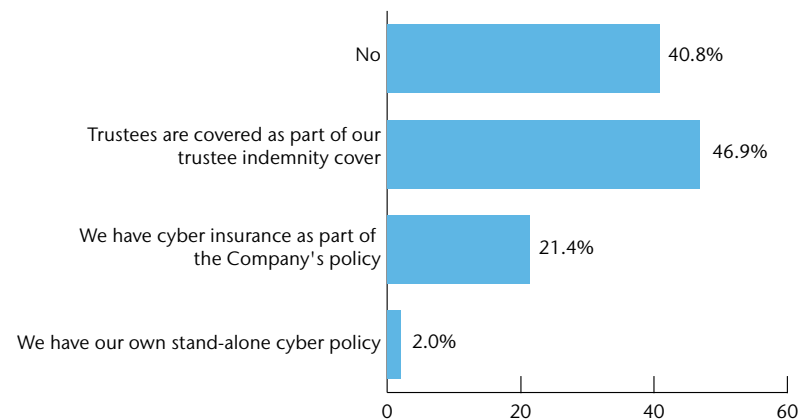
Next steps: Your cyber journey

Appendix



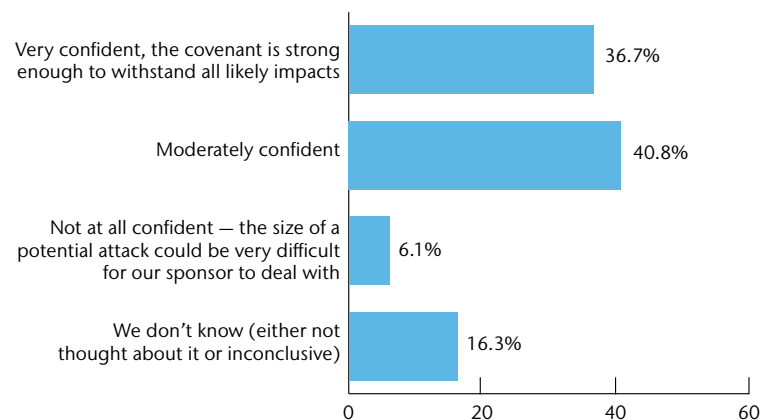
- Introduction
- Executive summary
- Profile of schemes
- The Pensions Regulator expects
- Part 1: Strategy, governance and documentation
- Part 2: Trustee risks
- Part 3: Scheme technology and processes
- Part 4: Third party providers
- Part 5: Your critical assets
- Part 6: Dealing with members
- Part 7: Incident response
- ▶ Part 8: Financial impact
- Next steps: Your cyber journey
- Appendix

### Is the scheme covered by any cyber insurance?



Our final question in the assessment was the only one asking for an opinion rather than a fact. In the end — as with most other risks — if the scheme suffers then the sponsoring employer is left picking up the bill. So we asked whether schemes were confident that their sponsor could deal with the financial impact of an attack on the scheme. The good news is that the majority felt that the answer was yes.

### How confident are you that your sponsor could support the financial impact of an attack on your scheme?



# Next steps: Your cyber journey

For most trustees, cyber threats are a new concept, and the thought of having to understand them and deal with them can be daunting. Add to that the fact that cyber issues cover almost every aspect of the pension scheme and it's hard to know where to start.

The Seek-Shield-Solve framework explained on page 6 can make the task a little easier to grasp, allowing trustees to focus on the three parts one at a time:

- Do I know what the risks are?
- Have I taken steps to mitigate them?
- Am I ready to deal with them if something happens?

It is also important that trustees do not feel that they need to do everything at once. Cyber resilience is a journey, and as our assessments show, schemes are all at different stages on that journey.

Some schemes have been working through their issues for a year or two and are now at the point of refining, revisiting and testing. These industry trailblazers have done it the hard way, creating policies where none existed, asking questions with no obvious answers, but steadily putting the pieces of a strategy together.

Others are just starting the journey — considering the basics or perhaps only just waking up to the risks. But while they may be behind the curve, the path to improved cyber resilience for pension schemes is now better trodden.

Wherever you are on your cyber journey, we hope this document has been helpful.

To complete your own scorecard, visit [www.aon.com/cyberscorecard](http://www.aon.com/cyberscorecard).

Introduction

Executive summary

Profile of schemes

The Pensions Regulator expects

Part 1: Strategy, governance and documentation

Part 2: Trustee risks

Part 3: Scheme technology and processes

Part 4: Third party providers

Part 5: Your critical assets

Part 6: Dealing with members

Part 7: Incident response

Part 8: Financial impact

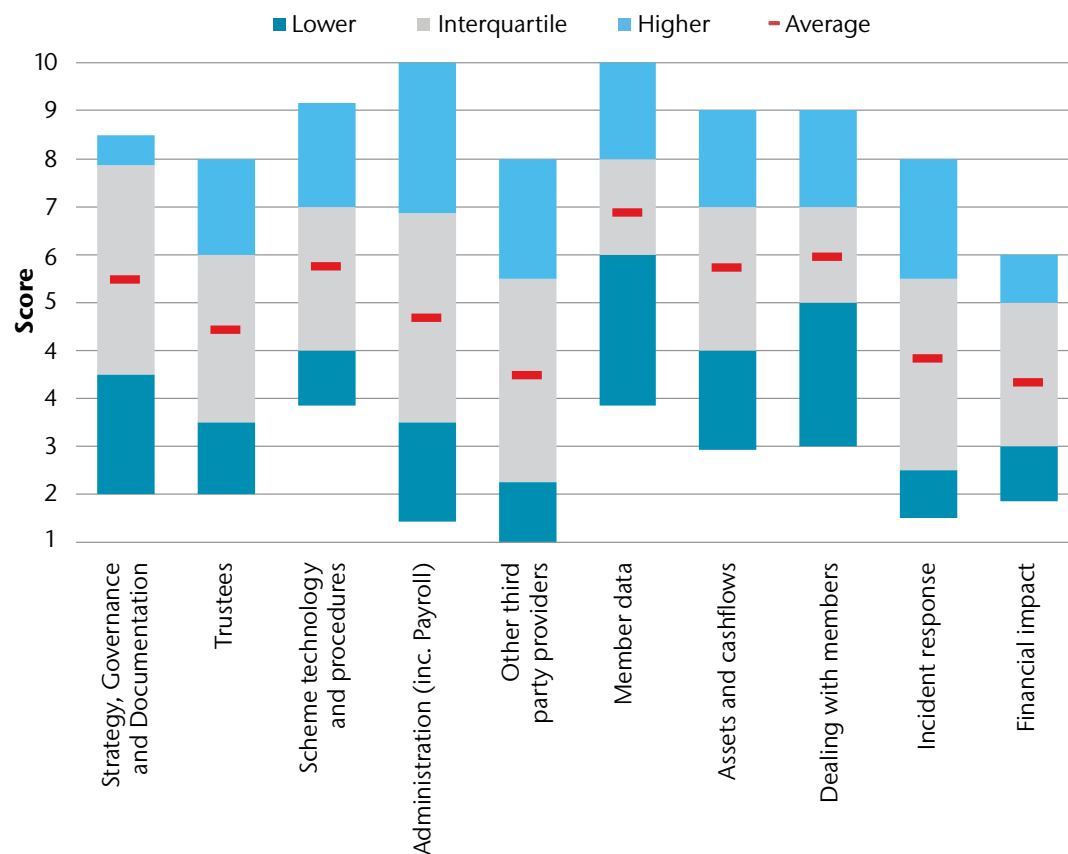
Next steps: Your cyber journey

Appendix

# Appendix: Benchmarking yourself with the pension cyber scorecard

As well as considering the individual questions and answers, all schemes undertaking this assessment were given a cyber resilience score, out of 100, broken down into a score out of 10 in each of 10 sections.

The graphs below show the range of scores, overall and for each section.



- The light grey area represents the 25<sup>TH</sup> to 75<sup>TH</sup> percentiles – 50% of responses are in that area
- The teal blue areas represent the 5<sup>TH</sup> to 25<sup>TH</sup> and 75<sup>TH</sup> to 95<sup>TH</sup> percentiles – 20% of responses are in each area
- 5% of responses are above the shaded area and 5% are below
- The red bar represents the average score

If you are interested in benchmarking your own scheme against this data, your free cyber scorecard can be obtained by completing the assessment at [www.aon.com/cyberscorecard](http://www.aon.com/cyberscorecard).

Introduction

Executive summary

Profile of schemes

The Pensions Regulator expects

Part 1: Strategy, governance and documentation

Part 2: Trustee risks

Part 3: Scheme technology and processes

Part 4: Third party providers

Part 5: Your critical assets

Part 6: Dealing with members

Part 7: Incident response

Part 8: Financial impact

Next steps:  
Your cyber journey

Appendix

## About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

For further information on our capabilities and to learn how we empower results for clients, please visit <http://aon.mediaroom.com>.

© Aon plc 2021. All rights reserved.

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Aon UK Limited is authorised and regulated by the Financial Conduct Authority.

[www.aon.com](http://www.aon.com)

