

# AON

➤ **Pension schemes and third-party providers:** Delegated functions, but not delegated cyber responsibilities **p78**

➤ **'Cyber VaR' and the path to cyber insurance:** How to protect against '1-in-20-year' events **p79**

➤ **The cost of cyber attacks:** Gill Wadsworth reveals the costs of cyber-attacks and how schemes can best protect against this risk **p80**

## Cyber focus: Rising to the challenge



➤ Aon associate partner, John Harney, and Aon partner, Paul McGlone

# AON

Sponsored by

# Pension schemes and third-party providers

## Delegated functions, but not delegated cyber responsibilities



Pension schemes rely heavily on third parties to provide critical services to their members. With this responsibility comes operational risk and the potential for huge impacts on scheme members and managers in the event of a cyber incident. Monitoring this is not an easy task, as a complex, ever-evolving risk, cyber challenges cannot be neatly reduced to a short checklist.

The potential of cyber risk is now firmly on The Pensions Regulator's agenda; their 2023 guidance stated that trustees "should seek assurance or evidence that the right controls are in place" for suppliers and those handling or managing systems. The guidance is clear that trustees "should not assume your suppliers and those handling or managing systems on your behalf have taken the required steps".

Thoughts may immediately go to third-party administrators, however, other providers could hold significant amounts of data or be critical to scheme operations. Furthermore, for many the sponsor of the scheme is also a service provider from a cyber point of view. Former service providers can also hold data that could have implications for the

scheme should they suffer a cyber incident.

### Doing nothing is no longer an option.

Most pension schemes will have little cyber expertise on the board, making the trustees' challenge - ensuring all providers (present

and past) are doing enough to protect scheme information - a daunting one.

- Step 1: understand the big picture. Who has access to your scheme data and assets; how is this information transferred between different parties? Understanding this enables trustees to better identify the potential impact on their scheme of an incident at these providers. Often this can be quite intuitive, so schemes do not need to carry out extensive mapping exercises if they feel their budget is stretched too thinly.

- Step 2: decide what assurances are required. Cyber assessments should be proportionate to the potential impact each provider poses, based on their operating relationship to the scheme. For instance, carrying out a review of a scheme administrator demands a more detailed approach than, say, an AVC provider.

- In our view, schemes do not need to use the same cybersecurity questionnaire across all providers; lighter touch questioning may be appropriate in some circumstances. For high impact providers, however, questioning should be more detailed, with responses to questions subject to trustee scrutiny.

- The final consideration is how

these assessments can be interpreted by trustees. Trustee boards with cyber expertise within their skillset are unusual. By their nature, reviews are technical and jargon heavy. In our experience, boards tend to need assistance from a cyber expert to establish whether the responses are in line with best practice or if additional measures should be sought from that provider. Expertise need not be expensive, and many can seek assistance from their sponsor. Others appoint third-party experts to manage a rolling programme of reviews. Whatever approach you take, output should include clear and concise reporting in a language that can be easily understood, with proportionate recommendations.

While this may seem onerous, I have seen how this approach can be established and embedded successfully in the scheme's risk management framework with the support of appropriate experts, and without disproportionate calls on trustee board time and resources.

Not only are these actions expected by TPR, but scheme members will also expect trustees to take this seriously. Understanding the scope of the risk is fundamental to building a robust, proportionate, risk-focused cyber resilience framework.

Unfortunately, no organisation is immune to cyber attacks, but by demonstrating alignment to best practice guidelines and being open to review and constructive feedback, schemes can be assured that their providers are taking the right steps to keep your information safe.

**For more information on Aon's Cyber Solutions email [talktous@aon.com](mailto:talktous@aon.com).**



Written by Aon associate partner, John Harney

In association with

**AON**

**H**ow much could a cyber incident cost your pension scheme? It is a question that could keep trustees awake at night, as most do not have a good answer. But that is changing.

The incident at a major administrator in 2023 caught the attention of the industry, with many schemes impacted. At the time it felt disastrous: finally, 'the big one' had hit. But in hindsight was it really that bad?

It was clearly a challenging situation, but in the end no data (that we are aware of) was sold on the dark web and no pensioner missed a pension payment. Day-to-day admin was impacted only for a short period; communication and identity monitoring was paid for by the administrator. Regulatory involvement was limited, and no schemes were fined. In short, it could have been a lot worse, and could have cost schemes a lot more had it panned out differently.

One of the concepts that pension schemes use regularly is Value at Risk, (VaR). In an investment context we typically use it to describe a '1-in-20-year' event: An event that is not the 'worst' that could happen but is unusual and damaging.

So, can we apply this to cyber risk, and ask: "What is my cyber VaR?" Put another way, what would the financial impact be on your scheme of a '1-in-20-year' cyber incident? It is a question that The Pensions Regulator also referred to in its 2023 guidance.

*"Understand the potential impact of a cyber incident on your members, the scheme, and where appropriate, the sponsoring employer. The impact assessment should cover multiple elements, such as operational, reputational, and financial impacts."*

*The Pensions Regulator, December 2023*

It is not a simple question to answer. Running stochastic models does not

# 'Cyber VaR' and the path to cyber insurance

## ▶ How to protect against '1-in-20-year' events



understand the risks that schemes face, and suitable levels of cover, it is now possible for pension schemes to secure their own protection should they wish.

In summary:

- Cyber risks can

have material financial consequences, which most schemes have not assessed.

- While the major administrator incident in 2023 was challenging, it was far from disastrous; it could have been much worse
- It is possible to assess the cyber risk for your scheme, to consider what a '1-in-20-year' event might look like, and to calculate your cyber VaR
- You can then decide what to do about it, whether that is just to accept the risk or look for options such as cyber insurance

For many schemes, cyber risk is still scoring high on risk registers. Perhaps these options could help boards with getting more comfortable with the residual risk.

**For more information on Aon's Cyber Solutions email [talktous@aon.com](mailto:talktous@aon.com).**



▶ Written by Aon partner, Paul McGlone

In association with

**AON**

make sense for this type of risk, and in any case, future cyber risk is very different to historic cyber risk. But it is certainly possible to construct realistic '1-in-20-year' scenarios and then assess the financial impact on a scheme. The outcome is likely to be a lot worse than the incident in 2023.

Once a scheme understands the potential risk from a cyber incident then the next question is: "What can I do about it?" And that answer is changing as well. Until recently schemes only had a few choices:

- Accept the risk, and hope it could be covered by scheme assets or a company bailout
- Piggy-back on the sponsor's cyber insurance
- Claim what you can through a pension trustee liability policy
- Hope you can recover costs from a provider through your contract

In practice, the latter three are all much harder than they sound, so most schemes have been left holding the risk. But over the past 12 months, cyber insurance for pension schemes has finally come of age. With suitable underwriting, insurers who



### Summary

- Cyber-attacks are becoming more frequent and costly, and trustees are directly liable for the risk.
- The Pensions Regulator expects trustees to have adequate protection plans in place.
- Outdated and ineffective cybersecurity makes pension schemes vulnerable to attack.



Protecting against cyber-attacks is an expensive business, but failing to take effective security measures can cost pension schemes an awful lot more.

In 2022 cyber-crime cost UK businesses on average £4,200, while the average cost to remedy is five times as much at £21,000.

This is something Capita found in March 2023, when the firm suffered a serious cyber security breach in which customer data was exfiltrated.

The attack affected thousands of pension members who had their personal data compromised and led to £25 million in costs, as well as reputational damage, potential loss of business and customers, increased regulatory scrutiny and investigations from the Information Commissioners Office and The Pensions Regulator (TPR).

And the threat from cyber criminals is only set to worsen. Cyber research firm Cybersecurity Ventures expects global cybercrime costs to grow by 15 per cent every year over the next five years, reaching \$10.5 trillion (£7.92 trillion)

# The cost of cyber attacks

## Gill Wadsworth reveals the costs of cyber-attacks and how schemes can best protect against this risk

annually by 2025, up from \$3 trillion in 2015.

In the UK, cyber is the fastest growing fraud with around £37 billion a year lost to all types, and of the £6 billion a year lost to pension fraud each year, the lion's share is now believed to be cyber.

And this could be a vast underestimation, since Pension Scams Industry Group chair, Margaret Snowden, notes the industry “does not collect enough data to be able to be sure of the figures, as companies and schemes do not always report ransomware attacks”.

### Ripe for the picking

Pension schemes are ripe for the picking for cyber criminals; holding trillions of pounds in assets and with deep reserves of member data make them a particularly attractive prospect.

Trafalgar House client director, Daniel Taylor, says: “Cybersecurity is one of the biggest threats facing pension schemes today. The message has finally sunk in; schemes hold massive amounts of sensitive data and significant sums of money, and many are still relying on outdated or cobbled-together systems that leave dangerous gaps. The industry is traditionally slow-moving, with legacy tech and data stores that create serious vulnerabilities.”

In December 2023, TPR issued updated guidance for pension scheme trustees on how to manage cyber risk to schemes. This was followed in February 2024 by a *Regulatory Intervention Report* on the Capita cyber security incident.

The watchdog is clear that trustees and scheme managers are responsible for protecting their members, and that they must have risk mitigation in place and

adequate procedures in the event that the worst should happen.

Aon partner, Paul McGlone, highlights how TPR expects every scheme to have an incident response plan that could be used in the event of a cyber incident, and to have tested it.

“The details of each plan will differ, as processes should be suitable for their specific scheme, structure, size, and people. For many schemes, the plan isn't so much about a rigid process as guidelines and checklists to refer to. Common elements of a plan would include some sort of severity assessment, an escalation process, guidelines on reporting, draft member communication, as well as emergency contact details and checklists to ensure that key tasks are not forgotten,” he explains.

TPR acknowledges the “amount of work involved in this type of exercise” but says trustees “should factor this in as part of effective contingency planning”.

Sackers partner, Olly Topping, says the level of resource needed will depend on the size of scheme and the number or different third-party providers it employs, but irrespective of the amount of commitment required, trustees must take cyber security seriously.

“Schemes are already very busy, and cybersecurity can a lot of resource, but the regulator feels, and we would agree, that this is a serious risk and requires the appropriate level of time and investment to manage if it is to be mitigated adequately.”

Topping notes that while larger schemes may have the resources to put cybersecurity in place, they may also have multiple third-party providers making oversight of all data and assets more complex.

Meanwhile smaller schemes, according to Snowden, “tend to keep their heads down or rely on third-party service providers”, but she notes that there is “no foolproof protection because cyber criminals are organised and sophisticated”.

“If criminals want to get in, they almost certainly will. A scheme should aim to be better protected than others; like a burglar alarm makes thieves move on to easier prey,” Snowden says.

### Prevention better than cure

Stephenson Harwood cyber lead, Joanne Elieli, says there are several prevention measures that pension trustees can enforce to ensure they are cyber resilient.

These include regular security audits and vulnerability assessments; robust data encryption; multi-factor authentication and strong password policies; and regular cybersecurity training for trustees, administrators and staff.

“Human error is the biggest vulnerability any organisation has and so regular, meaningful training can dramatically reduce this risk,” Elieli says.

Elieli encourages pension trustees to discuss their cyber security needs with their in-house and/or external legal counsel, together with their relevant technical team.

“The most effective type of support at a high level though is that which is collaborative, specifically between the legal and technical teams. You want your key stakeholders engaged too to ensure that best practices and cyber resilient measures are in place and being endorsed from the top down,” she says.

According to McGlone, prevention measures need to cover the trustees themselves, their various service providers, and the scheme sponsor.

“Most trustees start by reviewing the controls at their critical providers, typically administrators, and then work through other providers based on

potential impact of a cyber incident. But it’s important to include the sponsor in that assessment, as well as the trustees’ own controls. Having the most secure administrator is no help if the weakest link is a trustee using a Hotmail account on a laptop with no virus software,” he explains.

## “Cybersecurity is one of the biggest threats facing pension schemes today”

### Control, monitor, test

LawDeb director, Sean Burnard, says his independent professional trustee firm follows a strict cyber-security process.

“We have a mantra when it comes to cyber security: Control, monitor, test. It is this mantra that guides our behaviours and our recommendations to trustees. As the world becomes more digital, cyber presents an increased risk to schemes, trustees, and their members – it should be high on the risk register for schemes of all sizes.”

McGlone recommends that trustees have both preventative support and response support.

“Preventative support includes general cyber governance (e.g. setting up cyber policies and incident plans), specialist cyber expertise (e.g. assessing controls at providers) and legal advice (ensuring contracts are robust). Response support is quite different and can be practical support (e.g. project management), forensic IT expertise (e.g. if an incident needs investigating), legal advice (e.g. data privacy issues) as well as advice around member communication, media enquiries, credit monitoring services etc,” he explains.

TPR also expects trustees and scheme managers to have robust policies in place should the worst happen. Every scheme should have a cyber incident response plan that includes communication

strategies, legal and recovery procedures.

Snowden says: “The most important thing is for trustees to have a cyber expert on tap, whether directly or via cyber insurance. Doing your own thing when facing a cyber threat can often lead to a worse outcome, including you possibly going to jail. Ensure you have a plan on what to do if something goes wrong and have someone in charge of executing that plan. And keep on testing and replanning. Seems a lot, but the cost of doing nothing is much more than you can ever imagine.”

But the cost of such cybersecurity is an issue for some schemes, and since TPR places the burden of risk squarely with the trustees, they will need to find the resources to make sure they are protected.

Taylor says: “Tackling cyber threats isn’t a cost-free exercise. Schemes must recognise that it’s not just down to the administrator to plug every gap. Trustees need to be prepared to shoulder some of the costs and work together with their advisers in a spirit of cooperation. It’s a shared responsibility, and without the right level of investment and collaboration, it’s impossible to effectively defend against the growing cyber threat.”

In a world where cyber criminals are getting ever more sophisticated and the spoils from pension funds increasingly tempting, trustees will need to keep security both tight and responsive.

As Burnard concludes: “This is not a once and done. The cyber risk landscape is evolving as fast as the world’s technology, and trustees must regularly and thoroughly review their cyber approach to ensure they’re as prepared as they can be. The mantra holds true – control, monitor, test.”

Written by Gill Wadsworth, a freelance journalist

In association with

**AON**