Pension schemes and third-party providers

Delegated functions, but not delegated cyber responsibilities

Pensions 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.

Written by Aon associate partner, John Harney