

**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

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

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**