Paul McGlone is a partner at Aon

CYBER RISK, PENSIONS AND INVESTMENT

Cyber risk has risen quickly up the agenda for pension schemes. This article considers how schemes are dealing with the issue, and specifically how it applies to scheme assets.

From a standing start less than five years ago, the first guidance on dealing with cyber risk was issued by The Pensions Regulator in April 2018. In 2021, we have seen that guidance wrapped up in the Single Code of Practice, which is due to be in place early in 2022.

Faced with this new topic, which was not in their trustee training, many trustees struggled to translate the guidance into practical steps. But at its simplest, cyber risk can be dealt with in three stages, which in this article I will call seek, shield and solve.

- *Seek* involves considering what threats the scheme is exposed to. They will not be the same as other organisations. For example, an air traffic controller or a retailer have different cyber risks to a pension scheme.
- *Shield* is all about the actions that can be taken to protect the scheme against cyber threats. This is the core of dealing with cyber risk, with real actions across a range of different organisations.
- *Solve* deals with the consequences of an attack. If despite your best endeavours, a cyber incident occurs, how well placed are you to respond to it?

For a pension scheme the *seek* stage tends to highlight a relatively small number of risks, and these tend to be common to all schemes. In particular:

– Member data
– Scheme assets
– Administration and payroll systems
– Reputation (including the sponsor)

Most trustees focus on member data as the primary cyber risk. In this article, I have focused on the asset issues.

In the *seek* stage, a common action is to understand the flow of assets around the scheme. For smaller schemes that is simple and intuitive. For larger schemes, asset maps can track the various transactions, from the moment money enters the scheme bank account as contributions to the moment it leaves to pay members and where it gets invested in between. Data maps were created in the run up to GDPR, but asset flows are now seeing similar treatment.

As well as asset flows, the flow of investment or payment instructions is important, as a hacker intercepting an investment instruction is halfway to intercepting the assets. For example, in recent years we have seen an increase in fake investment instructions, often properly completed with real signatures, as well as fake invoices diverting money into hackers' bank accounts.

At the *shield* stage the primary question is what controls exist to prevent cyberattacks on assets. That means controls at investment managers, administrators, banks and custodians, as well as the trustees. Most appointed providers will have these controls, whether trustees realise it or not. And consultants usually include checks on cyber controls before including managers on their buy lists. But faced with guidance that recommends periodic checks, we now see trustees taking those issues more seriously, and asking for periodic updates from their providers.

Those questions are not just IT-related. For example, physical security and staff training to address the people side of cyber risk. One large scheme we worked with established that a large manager had no cyber insurance, which they were unhappy about. Whether it was directly due to the scheme's questions, or coincidence, after some discussion the manager did take out a cyber insurance policy.

Finally, the *solve* stage is about minimising damage. As well as having their own incident response plan, trustees want to see that their providers do as well. They also want to see contractual protection for incidents that may impact on their scheme.

In the short term, the part of the industry getting these questions most is scheme administrators. But in time we expect the same scrutiny to apply to anyone touching the scheme's assets.

The good news for anyone involved with investment is that most of this is not new. There are many other investors out there who have asked similar questions before. Anyone touching money has been dealing with cyber risk for many years, and most have solid controls and teams of staff to manage cyber risks.

The bad news is that this is newer for pension schemes, so there is not yet a standard way to deal with it. Until there is, investment managers, custodians, and anyone else involved with scheme assets will have to manage the many and varied requests which seem inevitable as the industry steps up its approach to this risk.