PENSIONSAge

Sponsored by

AON

Cyber insurance for pension schemes: *Cyber risk is a growing concern for the pensions industry. Aon associate partner, David Burwell, explores the challenges trustees face in securing adequate cyber insurance coverage* ***p38***

Meeting the pensions industry's cyber protection needs: *Pensions Age speaks to David Burwell about the benefits of a cyber incident insurance policy specifically tailored to the needs of pension schemes* ***p40***

Cyber insurance focus:

Protection for your scheme

Aon associate partner, David Burwell

AON

Sponsored by

Cyber insurance for pension schemes

Cyber risk is a growing concern for the pensions industry. Aon associate partner, David Burwell, explores the challenges trustees face in securing adequate cyber insurance coverage

Cyber risk continues to be a hot topic in the pensions industry and many schemes are working on managing this risk following updated guidance from The Pensions Regulator and the requirements of the General Code.

While most schemes have now developed a trustee incident response plan, and may have reviewed the cyber controls of their key providers, a recurring question asked by trustees is: "What about cyber insurance?"

Why is cyber insurance difficult?

Cyber insurance has been a tricky issue for the pensions industry. Trustees may want protection, and cyber insurance has been available to companies for many years, but a standard cyber insurance policy may not adequately meet the risk profile of pension schemes.

Corporate cyber insurance policies tend to focus on attacks on, or breaches of, computer networks owned or operated by the company. Pension schemes almost invariably outsource some, or all, of their operations to third-party providers. However, this does not remove their responsibilities as trustees. If a third-party computer system is compromised or becomes unavailable, or if data is leaked or corrupted, trustees will be expected by scheme members and regulators to respond rapidly and appropriately, irrespective of where the incident arose.

Until recently, trustees have looked either to Pension Trustee Liability (PTL) insurance or a cyber insurance policy taken out by their sponsor to cover some of these risks. Neither are attractive options for pension schemes:

- **PTL insurance** can provide broad cover for claims made against a pension scheme and its trustees, whether that arises from a cyber incident or not. However, it will not cover the scheme's own costs in responding to a cyber incident and will not cover any situation where there is no claim against the trustees.
- **A sponsor's corporate policy** sometimes includes cover for the pension schemes and should cover both first and third-party losses. However, it may be limited to cyber incidents affecting the sponsor's own computer networks. If the trustee is not a named policyholder then claims may be rejected. These policies can also be subject to large deductibles, meaning that an effective recovery will depend on the employer being willing and able to fill that gap.

Regardless of the existence of insurance, a pension scheme would seek to recover their losses from the third-party service provider if that provider was the cause of the incident. But this will be dependent on the terms of the contract which may be subject to limitation of liability clauses – particularly in the absence of fault – as well as on the provider's willingness and ability to pay. In any event, there is likely to be a substantial and unwelcome delay before matters are resolved.

A pension-specific solution

After many years of pension schemes being unable to secure effective cyber insurance, the insurance market now offers policies, underwriting approaches and cover levels that match the risk profile of pension schemes. These policies can be structured to include:

- **Breach response:** Cover for the costs incurred by a scheme in responding to a cyber incident or data breach. Where the incident affects the scheme's (or the trustee's) own computer systems, this may include the costs of restoring the system and its data. It will also include costs incurred by the scheme in response to the incident, starting with legal and technical advice and extending to the costs of taking the required action, such as notifying scheme members and providing credit monitoring or similar services.

A policy is also likely to include access (via a 24hr helpline) to the insurer's established panel of cyber response specialists to ensure that no time is lost in taking appropriate action.

- **Increased costs of working:** Where the costs incurred by a scheme are increased because of a cyber incident or data breach, for example if manual processing is required for a time, the cyber policy can also respond.
- **Liabilities:** Cover for the cost of claims made against the scheme and its trustees following a cyber incident or data breach. If these costs are also covered by a PTL insurance policy, consideration should be given to areas of overlap and which policy should respond first.

Cyber policies will not generally provide comprehensive cover for loss of assets, for example where funds have been misdirected following a cyber-attack or phishing event. Typically, a scheme will

need a dedicated crime policy if trustees want to insure against these risks as well.

Understand your scheme's cyber VaR

Trustees are typically comfortable with the concept of Value at Risk (VaR) and have been using this as a metric to quantify investment risk for many years. Most schemes will have a good idea of the level of downside risk they are exposed to from a 1-in-20-year investment shock and will have established processes for monitoring this. This concept can equally be applied to operational risk, such as cyber risk, and this is something lots of schemes are doing right now. This involves reviewing potential losses that the scheme might incur in a major cyber incident, to compare to any protection that is already in place and the willingness of the scheme (or sponsor) to accept that risk.

• If a scheme is planning to arrange cyber insurance for the first time, we recommend completing this type of assessment as a first step. That should include assessment of the key cyber incidents to which a scheme is exposed, including quantifying the potential loss in a range of circumstances, from a low impact incident through to a high impact incident.

• Identifying which risks are insurable and what type and level of cover is suitable.

• Establishing what contractual and insurance protections are already in place.

As well as being essential to establish the need for cyber insurance, such an assessment helps trustees to better understand the overall level of cyber risk they are running and is one of the often-overlooked requirements of the current TPR 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*

The good news is that this is not a complex or costly exercise. For most schemes, this will be a fraction of what is currently spent on other areas of governance or risk management, and a fraction of the annual cost of cyber insurance.

Once trustees fully understand their cyber VaR they can make an informed decision on whether cyber insurance is the right option for them. Even if the financial cover is not the driver, access to the specialist support and advice in the event of an incident can be invaluable. A helpful analogy is that of car insurance: All drivers will want their policy to cover the cost of replacing their car after an accident. However, the thing they may value most immediately is the emergency cover or replacement car that comes with the policy while they get back up and running.

An emerging area

Cyber insurance is still an emerging area for the pensions industry and trustees need expert advice to navigate the issues involved. Most schemes do not yet understand the financial exposure to a serious cyber incident and may only have limited support in place if something happens.

After many years of having no adequate access to cyber insurance, the market is responding to demand and there are viable options for trustees to consider, including access to support when you might need it the most. If you have not already explored this, now is a good time to do so.

Written by Aon associate partner, David Burwell

Meeting the pensions industry's cyber protection needs

Pensions Age speaks to Aon associate partner, David Burwell, about the benefits of a cyber incident insurance policy specifically tailored to the needs of pension schemes

We've all seen the spate of cyber attacks on businesses in the news lately. I'm sure most schemes will be concerned about a data breach at their third-party administrator. However, won't the costs of a cyber incident in that scenario be picked up by the scheme's provider?

For schemes outsourcing their administration, typically there will be some contractual protection about what might happen in the event of a serious data breach or a cyber incident. To some extent, if there's a big problem, the schemes can fall back on those contractual protections, but by no means will it cover all scenarios.

There is likely to be some additional costs that a scheme will likely have to pick up itself. So, the first thing is to understand what the full range of costs might be and who will bear them in which scenario.

You mentioned how contractual protection may not protect schemes against all the costs of a cyber incident. Is this where cyber insurance may help? Please could you explain how cyber insurance can protect schemes should a cyber attack occur? What circumstances are typically covered by this sort of policy?

Cyber insurance is supposed to capture as many as possible situations as can be envisaged by the scheme. Now, clearly, it's not going to be able to capture every single scenario under the sun. It is designed to capture some of the credible worst-case scenarios that a scheme might face, and that might be an incident impacting the scheme itself, or an incident which originates from a third party.

Additional advisory fees can be significant, particularly if you need to bring in specialist legal counsel, technical expertise or prepare additional member communications. These are all costs that very well could fall to the scheme. Actually, a lot of the value from the insurance policy comes from access to these specialist services that the insurer can provide.

Have many schemes already taken cyber insurance? Isn't this just something for the largest schemes?

It is a very new product; until very recently, there wasn't a cyber insurance policy designed for a pension scheme that a trustee board could buy. Instead, cyber insurance has been directed at corporates or similar institutions, which have a more typical business operating model than a pension scheme.

But now cyber insurance for pension schemes is available, it is something that all schemes should consider. We think it is appropriate for schemes of all sizes, because we think cyber is a ubiquitous risk that all schemes need to take steps to protect themselves against.

Cyber insurance can be affordable for schemes of all sizes but it may not be suitable for all. There will be several variables that impact the cost, but individual schemes can explore those and work out whether it would be a viable option for them, or whether they should continue to effectively self insure.

To expand on the cost element of that, I imagine cost may well be the main barrier preventing schemes from taking out cyber insurance. What might a typical cyber policy cost, and what kind of variables in the policy could affect the cost?

The market is still developing and the different flavours of this policy will evolve over time.

The variables may be things such as the amount of excess a scheme is willing to take on, and the maximum level of cover.

Also, the amount of additional services will impact the cost. For instance, how many additional specialist advisers might need to be on hand, given the size of the scheme and its complexity.

In terms of pricing these sorts of poli-

cies, we think that an annual premium might be in the region of £10,000-20,000 for up to £1-2 million of cover.

Other than cost, what else should schemes consider when weighing up the pros and cons of taking out cyber insurance?

The main thing for schemes to think about is their ability to withstand a major cyber incident.

Trustees may find that they have levels of cover and protection in different places. So although the simple question might be, can I not just insure this away, the answer is 'it depends', not just on the cost and the services you're effectively getting, but also where there might be cover already in place in the scheme's existing policies.

A scheme might have, for example, a trustee indemnity insurance policy. They might also have some contractual protections with third parties, plus some level of cover under the sponsor's cyber insurance policy.

So, the first thing to do is really to understand the level of risk the scheme is running and then conduct a gap analysis to see where there is still exposure in the event of a cyber incident.

From there, a scheme can determine where it makes sense to plug the gaps with a specific pensions cyber insurance policy.

So, if there is a very strong sponsor for a well-funded scheme, then just from a financial point of view, the policy might not be suitable. Or, if the scheme can already access the additional services that the policy would provide through the sponsor, such as technical expertise.

However, I think for most schemes, the premium price of having this extra cyber incident protection through an insurance policy is not going to break the bank.

Also, given that many trustees are thinking about managing schemes into their endgame, financial risk and investment risk is less important as they are well hedged.

Instead, attention is on operational risks, and the number one operational risk for most trustee boards will be cyber risk.

So, the option to insure that risk and have access to all those bells and whistles that come along with that policy is probably a sensible spend for a trustee board. It provides peace of mind and having a policy like this is good governance for trustees.

Why has it taken so long for the market to provide a cyber insurance policy tailored to the needs of pension schemes?

We have been giving cyber governance and advice to pension schemes for around eight or nine years. From day one, trustees were asking us what can be done about cyber insurance, whether they could simply buy a policy that insures the scheme. Unfortunately, that product just hasn't been out there to buy until now.

I think that was due to a slight knowledge gap in the insurance industry as to how pension schemes work and operate. Underwriters found it difficult to get to grips with how pension schemes operate, with their questions more geared towards traditional corporates.

Therefore, we have had to work very closely with brokers and underwriters to develop a cyber insurance product and I'm pleased to say the market can now offer a policy that is appropriate for pension schemes.