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