Preparing for the worst

Just like every other organisation, pension schemes need to manage potentially disruptive operational risks, and be prepared to respond to a crisis that could threaten a scheme's operations and its members' wellbeing. David Adams looks at the steps trustees, managers and employers need to take to ensure a scheme is ready to respond when a crisis strikes

Summary

- Pension scheme trustees, managers and sponsoring employers need to work continuously to identify and manage operational risks that could create significant problems, or a major crisis, for the scheme.
- Risks include the disruption caused by unusual events such as a pandemic or extreme weather, but also cyber risks, which may affect the scheme directly, and/or operations of administrators and other service providers, possibly leading to the theft of members' personal data.
- Trustees, managers and employers must proactively ensure that service providers have taken steps to mitigate any risks that could affect the operation of the pension scheme.
- DB scheme trustees and managers also need to be aware of and seek to manage operational, financial, or regulatory risks that might adversely affect a sponsoring employer, possibly creating another type of crisis for the scheme.
- The Pensions Regulator has created extensive guidance on different aspects of risk management, which is also addressed in its General Code. This should be followed, along with expert advice, when planning how to protect the scheme in the event of a crisis.

We live in an unpredictable and sometimes hazardous world; pension schemes are just as vulnerable as any other organisation to a variety of potentially disruptive and damaging operational risks.

Some, like the impacts of a pandemic, extreme weather, or social unrest, are at least relatively unusual. Others, such as cyber risks, have become a constant source of possible problems, which might be caused by mass system outages, or by hacking or malware removing data from IT systems. Managing and mitigating these risks is difficult because they may disrupt the work of service providers, particularly third-party administrators, upon which the scheme relies.

We saw an example of this in spring 2023, when outsourcing provider and scheme administrator Capita was hit by cyber-attacks that led to two significant data breaches. About 90 Capita clients were affected, including multiple pension schemes that were forced to tell members that their personal data, such as bank details and/or passport photos, might have been extracted from Capita's systems. By January 2024 more than 5,000 people had joined a group action lawsuit against Capita seeking compensation.

The Pensions Regulator (TPR) concluded its investigation into the case by stating that the breaches demonstrated the importance of "ensuring that trustees or managers of pension schemes and their providers have robust cyber security and business continuity plans in place".

Another group of ever-present risks are linked to the fortunes of employers that sponsor DB schemes. The first step trustees should take in addressing these risks is to familiarise themselves, if they have not already done so, with TPR's guidance for protecting schemes from sponsoring employer distress.

PwC head of the pensions employer covenant and restructuring team, Mark Jennings, says the way he and his colleagues advise DB scheme trustees has changed, in part because the nature of risks affecting employers has changed, but also because scheme funding levels have improved, meaning many are now preparing to move towards an endgame.

"A key issue for many trustees now is making sure that the sponsor is able to stand behind the scheme for the next five to 10 years, rather than a focus on cash contributions," says Jennings. He highlights the potential for employers to be adversely affected by risks linked to ESG or climate-related regulatory or legislative changes, for example.

Use guidance and expert advice to plan a crisis response

TPR has produced detailed guidance for trustees on identifying, monitoring and assessing risks, including guidance on continuity planning. It also stresses the importance of understanding the processes that service providers, particularly administrators, put in place to manage the risks that might disrupt their operations.

"We do not expect governing bodies will have the power to eliminate all risks – that's not realistic," says TPR policy lead, Nick Gannon. "But we do expect them to understand the risks facing their scheme and the power they have to effectively manage and mitigate those risks. Where governing bodies conclude they do not have the knowledge or understanding necessary to do this they should seek … expert support and … appropriate advice.”

Trustees must ensure service providers have adequate cyber risk management processes and business continuity plans in place. They must not simply assume that will be in place, says Pensions Management Institute (PMI) vice-president and non-executive director, Rosie Lacey: “Employers should ensure … the provider has … a cyber security plan and a business continuity plan.”

There are other potential risks that trustees or employers may not have considered, says Barnett Waddingham head of resilience, Karla Gahan. They include key person risks: What happens if an important individual, such as a professional trustee who usually chairs the board, or a lawyer who has in-depth personal knowledge of the scheme, is not available, because of illness, for example, when a crisis occurs?

Trustees or employers need to consider such questions as they determine which individuals will form a response team to guide a response to a continuity incident or a crisis. Such a team needs more than a couple of members, says Gahan: “If you only have one or two people they will burn out.” She suggests that ideally a team would contain five or six people, including a lawyer and/or PR adviser, if possible – perhaps engaged on a retainer basis to try to ensure their availability when needed.

Gahan also thinks not enough attention is always paid to the importance of communication with members, other stakeholders or the wider public in the event of a crisis.

“Members, including retirees receiving pensions, may use email or social media channels, so you need to use every channel available, rather than just sending letters,” she says. Gahan suggests communications plans are based in part on consultations with lawyers and PR advisers, if possible, but also says that “even having thought about this is a great first step”.

Consultancy and investment governance provider Avida International advises some of the UK’s largest pension schemes on continuity planning and crisis management. Founding partner, Paul Boerboom, says he and his colleagues advise schemes to “try to imagine the unimaginable” when planning.

“Do your utmost to come up with scenarios that are hard to imagine and haven’t happened in the past,” he advises.

He also urges trustees to try to make improving risk management and planning for crisis management part of a scheme’s organisational culture.

“It’s easy to ensure you’ve got risk registers and risk mitigation measures at all levels, but does the organisation have risk management and crisis management in its DNA?” he asks.

> **“Effective risk management demands constant attention”**

Test, test, and test again

The other vital measure to take is to test the plan rigorously. “Train yourself, with risk and crisis management exercises, wargaming and simulations,” says Boerboom.

Gahan also stresses the importance of such exercises. “No plan will ever be perfect – you will always find something new when you test it,” she says.

There will be more work to do in the event of a crisis. The regulator’s report on the Capita breach lists key steps trustees should take in the event of a cyber security incident, including ensuring clear communications with an employer, administrator and any other service providers to build and share a picture of how the scheme and its members might be affected, or are already being affected.

Payment of benefits, retirement processing and bereavement services should be prioritised. If a data breach has occurred, trustees should notify the regulator and the Information Commissioner’s Office (ICO). Trustees must establish whether key services can still be operated safely, restoring those operations when it is safe to do so. They must also put care and effort into communication with members, signposting them to appropriate guidance so they can take any necessary actions to protect their personal information, and avoid any potential scams. Finally, the scheme should monitor carefully any increase in, or unusual transfer requests.

How well-protected are the UK’s pension schemes against these sorts of risks? Gahan says levels of preparedness for a crisis “vary dramatically” from one pension scheme to another. “Some are awesome, some are really shocking,” she says. “It’s a very mixed bag.”

Jennings thinks there is now “an increased focus on risks” overall, among trustees and others with responsibility for managing schemes, but that this tends to be true most often within larger schemes, or at least those with the greatest resources at their disposal.

Boerboom also thinks some of the UK’s largest pension schemes “have got their house reasonably well in order”, in terms of continuity and crisis management planning; while smaller schemes are more likely to be over-reliant on measures put in place by service providers. But he thinks every scheme would benefit from more use of exercises to test plans and preparations.

Speaking for the regulator, Gannon stresses the need to assume a need to continuously repeat and refine risk management and crisis management planning.

“Some risks will diminish with time, while others will grow, and new ones appear,” he says. “Effective risk management demands constant attention.”

Written by David Adams, a freelance journalist