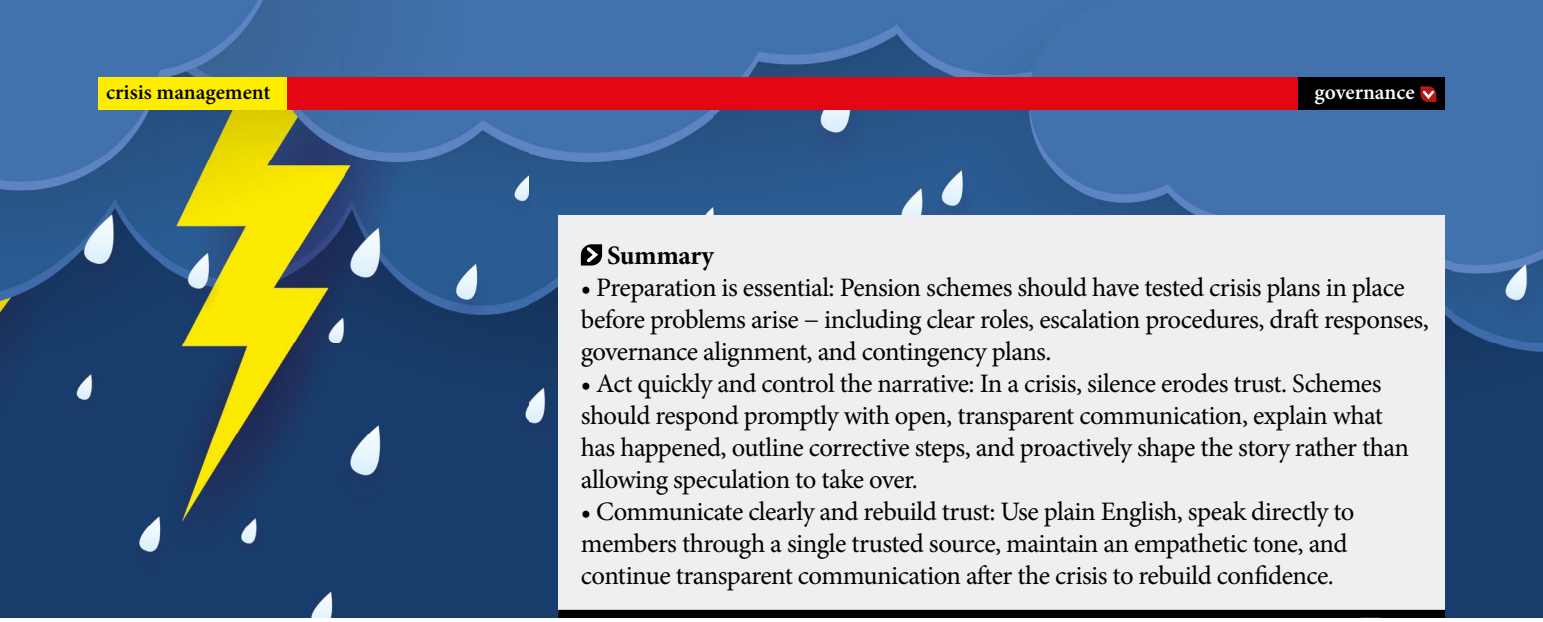

Summary
• Preparation is essential: Pension schemes should have tested crisis plans in place before problems arise – including clear roles, escalation procedures, draft responses, governance alignment, and contingency plans.
• Act quickly and control the narrative: In a crisis, silence erodes trust. Schemes should respond promptly with open, transparent communication, explain what has happened, outline corrective steps, and proactively shape the story rather than allowing speculation to take over.
• Communicate clearly and rebuild trust: Use plain English, speak directly to members through a single trusted source, maintain an empathetic tone, and continue transparent communication after the crisis to rebuild confidence.

When the storm hits: How pension schemes can protect trust

With cyber threats a key risk, crisis preparedness is no longer optional. Industry specialists outline five essential steps for staying in control when the unexpected happens

If permaculture was part of the zeitgeist in the 1970s, today, we are surely living in the era of permacrisis. The news is available 24 hours a day, and comes from a wide variety of sources, some more trustworthy than others. Today, news stories are touchpaper; they can ignite what often feels like a starkly divided world.

The possibility of a data security breach is the crisis scenario that is most likely to cause insomnia for pension scheme trustees, says Sackers partner, Joanna Smith. "Cyber is coming up as the number one thing people are worried about," she reports.

After all, people's sensitive personal data and money are two extremely emotive subjects, and there are few areas of life where the two overlap in the way that they do in pensions.

In recent years, many other crises have reverberated through the pensions world. Anything that affects pension schemes operationally is a big deal, from the liability-driven investment (LDI) crisis to the Covid-19 pandemic.

As WTW senior director, Lou Harris, points out: "For those members who have pensions in payment, if operations are slowing down or affected, that's a major crisis."

As many schemes prepare to submit their Own Risk Assessments (ORAs) for the first time in spring 2026, crisis management will be top of mind for trustee boards.

So, what happens when your pension fund or company becomes the centre of the storm? Here are five principles to bear in mind.

1. Preparation is key

"The age-old adage is true here: Fail to prepare, and prepare to fail," says Galene + Partners founder and PR specialist, Georgie Rudkin. "There is a massive piece of work that needs to happen way before a crisis unfolds, which is general crisis scenario planning. Companies sometimes forget this because it can be very uncomfortable. Not intentionally, but sometimes when there are disconnects between leadership, a lot of the problems that might arise do not come to the surface early enough."

But how can you prepare for the Donald Rumsfeldian 'unknown unknowns'? "It's good to have a plan, whatever the crisis is," says Harris. The experts agree that some principles will hold true, irrespective of the nature of the emergency. Here are a few pointers.

Rudkin says: "Working out who does what in a crisis is super important. What is the escalation plan when you get that first call, who should be in the room, how do you contact people, what is the code word you need to use? Time is of the essence, and you need to be prepared for that."

Prepare initial drafts responding to the most likely scenarios you may encounter and keep them updated as the world changes. Then, roleplay those scenarios in real time. That will help you to spot any flaws or gaps in your plans.

This is echoed by consultancy Untamed co-founder, Karen Quinn. "Any plan needs regular testing, not drafting and filing. And it needs an explicit owner. Without this, it probably won't work under pressure."

Some other practical points to consider: Who will take charge of what

media channel during a crisis? Know who needs to be informed in which crisis scenario – whether that is The Pensions Regulator or the Information Commissioner's Office, for instance.

Smith suggests that schemes should consider eventualities like what happens if the internet goes down. Do key stakeholders need a printed out copy of the crisis policy and a call tree? If so, where will they store it?

Assuming the internet is up and running, it's a good idea to have a quick way for the emergency committee to communicate. "Lots of our clients have set up WhatsApp groups for emergency planning," adds Smith.

All this should be underpinned by a robust governance procedure, agreed by a committee, which is consistent with the scheme's wider governance, including its Articles of Association, points out Smith.

2. Take control of the narrative

The worst has happened and there's a crisis unfolding, with your scheme or company at the centre of it.

The first lesson is to say something wherever possible, KBPR client director, Kate Boyle, says: "As a general principle, I'm a strong believer in open and transparent communication wherever possible. Of course, there are times and circumstances, particularly where legal or regulatory sensitivities apply, where full disclosure is not possible. However, where schemes can 'own' the issue, explain what has happened, outline the steps being taken, and demonstrate control of the situation, that approach almost always leads to better long-term outcomes. It's far better to shape the narrative than to let it be shaped for you."

"A data security breach is the crisis scenario that is most likely to cause insomnia for pension scheme trustees"

Responding swiftly is critical, Quinn agrees, adding: "Silence damages trust, faster than honesty about an issue. If there's a void, it will be filled and you'll lose control."

3. Speak directly to members, in plain English

What exactly should you say? While there may be technical explanations for a data breach (for example) it is important not to get bogged down in the detail. Rudkin says: "Talk in plain language. Nobody needs to know the ins and outs and complexity of the malware that was on the system, the CTO coming out and explaining XYZ security protocols – people don't want that. Explain in simple terms what has happened and what you are going to do to fix it. No corporate jargon. When companies are unsure, they bury uncertainty in the language – but people see straight through that."

4. Make sure your information comes from one, trusted source

Ideally, you would already have built a regular communication channel with members, so that they see you as a trusted source of information, says WTW senior associate, Oshin Sharma. "Be sure that before a crisis arises, you have communicated with your members that this is their source of truth and that if something happens, this is where they should go to for their news updates.

Be careful with social media, she adds; engaging in a conversation can create more questions and inconsistency. "Members may use social media, and you might have a team that monitors the chatter going on on those platforms. But use your scheme's website as a way of updating them or giving them answers."

It is a good idea to train trustees, who may have their own relationships with journalists, in what to say should a crisis happen. Trustees should know the point of contact for journalist enquiries and be confident in what they can – and crucially, cannot – say, explains Sharma.

Sharma finishes: "It's important for the trustees to put themselves in the members' shoes. If *[a cyber incident]* happened to you, you'd probably be feeling panic. So, one of your key principles should be that your tone of voice needs to be empathetic and really reassuring."

5. Once the storm has passed…

It will take time to recover, but honesty and clarity will be your friends. Rudkin finishes: "Once you're out of the storm, don't think it is going to go away. You are going to have to keep rebuilding that trust. Don't bury it under the carpet once it has happened, use it as a case study for how you are learning, growing and changing the business, modernising systems and not shying away from the fact that there has been a problem in the past."

Written by Louise Farrand, a freelance journalist