AON

Cheryl Payne, HSBC Pension Bank Trust (UK) Trustee Chief Risk Officer

Laura Blows, Pensions Age Editor

Paul McGlone, Aon Partner

Cyber risk

Pensions Age talks to Aon partner, Paul McGlone, and HSBC Pension Bank Trust (UK) trustee chief risk officer, Cheryl Payne, about cyber risk in our latest video interview

What lessons have been learnt since the Capita cyber incident a couple of years ago and how has the industry changed its approach to cyber risk in the two years since?

Paul McGlone: The biggest thing that we've seen is more attention being paid to cyber risk.

Clearly, a lot of work went on at the time of the Capita incident, and The Pensions Regulator (TPR) was quite heavily involved. At the end of 2023, it put out new guidance around cyber risk.

TPR had already put guidance out a few years earlier, but the new guidance went into more detail. It linked it to things like the General Code and made it much more of an obligation for trustees to act.

We have seen a lot more provider reviews taking place – looking at third-party providers, understanding their cyber controls, understanding what they do with data, what they do with the assets. Also understanding things like supply chain risk. We have also seen a lot more focus on where the data is.

When a pension scheme has an incident and is named, the name of the sponsor is clearly part of the name of the scheme, so sponsors have become a lot more engaged.

I think one of the things people recognised at the end of the Capita incident was that it could have been an awful lot worse.

Although it felt terrible at the time, a number of things that could have happened didn't happen. Schemes have started to think: 'Well, maybe we got off quite lightly there – and how well prepared are we if something worse were to happen?'

Cheryl, from a scheme perspective, what tips or advice would you give – and for the providers themselves?

Cheryl Payne: It's always about how you're working with your third-party providers and your suppliers and really getting to understand what they do for you; how they do it.

So, it is understanding who has your data and what they do with it.

And then think about your supplier reviews – and think, do I need the same level for all of them? Probably not.

If I have suppliers who have got my data that's moving, then I'll have a far more in-depth review undertaken. And that, for me, means I can use the money that's available to me to protect us in a really good and efficient way.

And then working with our suppliers in partnership, really learning off each other, I think that's key.

When you've got a number of reviews coming in, see what you can – professionally and with integrity – do to help each other get stronger and safer day by day.

Paul, you mentioned that things could have been worse. Just how much worse do you mean?

McGlone: It could have been a lot worse. For example, every pensioner still got paid.

There were data issues, but to the best of our knowledge, data was not actually sold on the dark web or used for fraud, for example.

Systems went down, but for a very short period of time. Backlogs were generally dealt with quite quickly.

There was a lot of member communication, and fraud monitoring, and for a lot of schemes these were managed by Capita and paid by Capita.

So, all of the stuff that could happen – no pension scheme had to pay a ransom, for example – all of these things that keep people awake at night didn't happen.

Therefore, what schemes are now starting to think about is: What if those things had happened? What would a really bad event cost me?

Then you can start to think about things like cyber insurance.

If you know that for your 1,000-life scheme, a really bad incident could cost, say, £500,000, you can start to think: Do I need to insure that half a million pounds? Or am I confident my sponsor could deal with the half a million pounds?

Even if you don't need the financial protection, what about all of the incident response stuff?

Those are the sorts of things people are thinking about, and it's all triggered by the question: How much worse could it be, and are we ready if that was to happen?

How important is the role of the sponsor?

Payne: Working in collaboration with the sponsors is crucial. Every sponsor will have different things they can add to the party.

If you're in the financial services industry, for example, you can really make use of their intelligence, their systems, how they do things.

Even though it might be different for you as a pension scheme, you can take that core information and tailor it.

In every industry, there'll be something the sponsor can add. There will be diversity of thought within the sponsor, so being collaborative and cohesive is really important.

Paul, how do you keep cyber risk high on trustees' agenda?

McGlone: One of the things we keep coming back to is incident simulations, also known as war games, or a fire drill.

It's very easy to write things down on paper and ask trustee boards to read it but it's deathly dull, if you're not careful.

But when you take them through a live incident and say, 'this has just happened, how are we going to respond?' with the sponsor in the room, the providers in the room – you're having an active conversation through a live incident, that's what brings it to life and gets people engaged.

If at any point cyber seems dull – run one of those sessions, and it won't seem dull anymore.

Cheryl, do you have experience of that?

Payne: I do indeed, and I couldn't agree more with what Paul says.

You may start off by testing your own incident response plan, and then you might move on to having a third party with you and doing it together.

But what it does do is bring all the parties around the table in a really safe environment, giving that time and space to be curious, to be inquisitive, and to explore how it would feel if this happens.

You can have a lot of fun with it at the same time, but it can really draw out where you need to focus.

What do you think the areas of focus will be regarding cyber risk in the next couple of years?

McGlone: We're seeing more cyber threats because of AI. In the two or three years since ChatGPT was launched, we've seen phishing emails go through the roof because they can be created more easily.

But at the same time, you have AI defensive cyber controls as well.

So for example, imagine you're working from home one day, and your computer suddenly disconnects itself from your corporate network. Someone phones you to say, "we think you've got some malware on your computer".

Now, you may think that's a scam – and it may be a scam – but actually, it could be that the AI in your computer has recognised unusual behaviour, thinks it may be a cyber threat, and has isolated you from the network to protect the rest of it.

These things are happening all the time, and they continue to evolve.

So I think how AI is used in cyber – both as an attack vector and as a defence – will really change in the coming years.

Payne: Quantum computing and what difference that's going to make in the industry and in financial services at large.

That, for me, is something we're all going to have to start upskilling ourselves and thinking about.

There will be opportunities, just like with AI, but there will also be threats. And we need to be ahead of that.

This is a shortened and edited transcript. To watch the video in full, please visit pensionsage.com

In association with

AON