CYBERCRIME

In the wrong hands

Whilst the reporting of cyber security attacks remains low amongst pension schemes, the risks are increasing. Natalie Tuck **reports on how pension schemes can protect against this threat**

WRITTEN BY NATALIE TUCK

In a time when Europe appears to have become divided, the Covid-19 pandemic has shown the sense of community and unity amongst citizens across the continent.

Although borders have been shut, and national efforts have taken over, the global science community is working together to help discover a vaccine for the world's citizens.

That's why it was such a shock to hear of cyber attacks on labs involved in Covid-19 research. But, it is also a stark reminder that valuable information serves as a hook that draws in cyber criminals. In a report last year, the Thinking Ahead Institute labelled cyber warfare as one of the world's top 30 risks.

Pension funds, with masses of personal data about their members, are not exempt from this risk. Redington chief technology officer, Adam Jones, notes that the biggest risk areas for pension funds are through data loss and theft, as well as the onward sale of member details.

"This is a risk for data held by the scheme, but also processes being carried out by third party administrators, actuaries and consultants on their behalf. Where data is personally identifiable, there is also a GDPR risk. Furthermore, there is a threat to assets and cash, however this isn't held directly by the pension scheme, but rather custodians and banking partners," he says.

Most recently, the European Insurance and Occupational Pensions Authority (EIOPA) warned that since the outbreak of Covid-19, schemes are at an increased risk of exposure to fraud. "This includes cyber security and data protection, in particular, relating to staff working remotely," it stated.

Prior to the outbreak, pension schemes had not reported any significant cyber attacks. Aon's *Global Pension Risks Survey 2019* found that in the UK, over 95 per cent of respondents have not been affected by cybercrime. This does, however, mean that 5 per cent of schemes have been affected, and as Aon warned, a figure that is unfortunately likely to increase.

In other countries surveyed, Aon found that no schemes, so far, have reported any cyber incidents, but the risk of an attack is on their radars. So what are schemes doing to prepare and protect against potential cyber attacks?

According to Aon's survey, in Switzerland, half of the respondents have documentation in place and policies and emergency procedures. The remaining schemes plan to put this in place during the next 12 months (by September 2020). However, only one third have carried out a stress test of their organisation/infrastructure, or a simulation type 'war game'.

In Germany, attention has mainly focussed on the secure data transfer to service providers, such as the actuaries, according to Aon. Companies have also started to implement additional measures for risk management such as cyber training for those responsible or comprehensive assessments of the threat risk.

Insurance is another option; in Germany, two thirds of respondents have already assessed their existing cyber risk and taken out respective insurance policies. However, it is not yet possible to take out specific cyber insurance policies for occupational pension schemes in Germany. Aon suggests schemes should verify whether it is possible to include a certain cyber protection in existing insurance policies.

More generally, Jones adds that good governance is key in mitigating cybercrime risks. "Forward-looking pension schemes will have information security and associated issues forming part of their governance framework," he says.

"As with any risk-based framework, it's important to understand the current risk exposure. This can be done via a top down review of your business structure and third-party relationships, or equally with a bottom up review of processes. Once you have a good understanding of the risks, it's important to understand mitigants and implement these wherever possible." ■