Legal

Disaster, all member records lost to hackers!

By Aaron Dunning-Foreman, Associate, Sackers LLP

This is not a headline you would want to wake up to ... Figures published last April set out the average prices cyber criminals are thought to be paying for personal data, with email addresses worth between 75p and £3, proof of identity £46, and bank account details around £167.

With that in mind, a pension scheme is the dream target for cyber criminals. Many schemes have tens, if not hundreds, of thousands of member records, encompassing email details, bank account details, dates of birth, addresses, and proofs of identity.

I will not attempt to calculate the dark web value of an average size scheme's data. But clearly, a cyber breach could have severe consequences for a pension scheme and its members. Beyond the potential losses to members and risks of claims and fines, knock-on service disruption and reputational damage to the scheme and employer are highly likely.

It is not surprising then that pension scheme trustees (and managers) have a variety of obligations, from a variety of sources, when it comes to cyber security.

The Pensions Regulator (TPR) has been paying increasing attention to the matter of cyber security in recent years. In April 2018 it published its 'Cyber security principles for pension schemes' Guidance, making it clear that TPR considers cyber security a vital aspect of the internal controls that trustees are required to operate.

Obligations also flow from the General Data Protection Regulation (GDPR), with severe penalties imposed for certain breaches. The GDPR's core principles oblige trustees to ensure 'appropriate security' of the data for which they are responsible.

Cyber resilience: steps schemes should be taking

Trustees should be looking to take the following precautions as a minimum, to build their 'cyber resilience':

1. Ensure you understand the cyber risks facing your scheme, record the issues on your risk register and keep them under regular review

2. Put in place, and test, effective and proportionate controls to mitigate the risks identified. Ensure that your service providers also have appropriate controls in place. This is not just about security software, but also about working systems and processes to protect scheme data

3. Ensure relevant people fully understand their roles and responsibilities: undertake training, train others, and keep abreast of industry standards in the area

4. Put in place an incident response plan which sets out how, when and by whom you will be notified of a cyber breach, what you and relevant third parties will do to investigate and mitigate a cyber breach once it has been detected, and when and how you will notify third parties of any incident, including the Information Commissioner's Office, TPR, and scheme members.

Cyber security is a rapidly evolving challenge, and one that all organisations and individuals need to manage on an informed and ongoing basis. Pension schemes should make sure that it is, and remains, high up on their agendas.