Cyber security

for the 21st Century pension scheme trustee

In the 21st century, personal data is an increasingly valuable commodity, and pension schemes, by their very nature, hold an enormous amount of it. This article considers the challenges "cyber security" poses to pension schemes and sets out some practical steps for trustees.

Why look at cyber security now?

With the General Data Protection Regulation (GDPR) coming into force on 25 May this year, pension scheme trustees are busy updating their policies and processes ready to comply with the new legislation. As "data controllers" under the GDPR, trustees are required to take "appropriate technical and organisational measures" in respect of personal data that they hold. Having appropriate cyber security measures in place is an important element of data protection compliance, so it is an ideal time to consider it in more detail.

The Pensions Regulator has also reminded pension schemes of the need to be aware of the issues and challenges that cyber security presents for them.

What challenges does cyber security present?

Technology has enabled scheme administration to be automated, and to be shared quickly, but while the benefits of technology are clear, the risks that it introduces cannot be ignored:

+ **Loss of access to data and administration systems:** hacks, malicious viruses and system failures could disable an administration system and prevent access to the data and processes which are needed to provide the correct benefits to the right members.

+ **Data can be stolen or hacked.** While scheme administration systems have not yet been the target of a hack, the information available could be valuable to fraudsters. For example, personal data could be used for identity theft, and that data, combined with account information, could give access to members' bank accounts and other financial assets.

+ **Human error from administrators and others involved in running a scheme:** for example, steps in checks used when identifying members could be missed; information could be shared with the wrong person; [devices] and memory sticks can be lost.

Serious consequences of such breaches could include:

+ service disruption
+ fraud and financial loss to members
+ regulatory action, fines and claims from members
+ reputational damage for the scheme and the employer
+ time and financial costs to the scheme in addressing issues, reporting to the Information Commissioner and communicating with members
+ loss of member confidence.

Practical steps for managing cyber security and its risks

Pension scheme trustees are required to understand potential risks to their scheme and to adopt risk management measures that are appropriate and proportionate.

+ Identify when, where and how data is used and who is using it.

+ Carry out a risk assessment. This should include considering how trustees, administrators and advisers could be party to a breach or security failure. In practice, where schemes have experienced data security incidents, these often stem from human error rather than external attacks.

+ Assess safeguards that are already in place and review whether further safeguards, information from providers, and/or any other steps are required.

+ Establish a cyber and data security policy that outlines the trustees' approach to cyber security, steps that would be taken in the event of a breach (an incident response plan), and ongoing plans for reviewing and monitoring cyber and data security.

+ Ensure that the trustees' **risk register** addresses cyber and data risks.

Safeguarding measures include:

+ the use of passwords and encryptions

+ ensuring those with access to scheme data understand the importance of data security and the role they play in maintaining it

+ considering whether, and for how long, data needs to be shared or stored

+ where data is accessed electronically, checking whether users' systems are secure

+ checking that providers' contracts include terms relating to data security, and addressing any gaps.

Katy Harries
Senior Associate, Sackers