ALLEN & OVERY

Cyber risk: practical actions to improve data security

Trustee processes

Trustee papers may contain a range of member information, including sensitive personal data (eg in relation to ill-health applications).

- The simplest way to improve data security is to minimise transmission: do trustees really need identifying member details, or could information be anonymised to reduce the potential consequences of any data loss?
- Trustee papers will be more secure if kept on a trustee portal with password-only access than if they are circulated by email or in hard copy.
- Pensioner trustees, in particular, may rely on insecure home email addresses, which can easily be hacked. Ask the scheme sponsor to provide work-based emails for all trustees within the organisation's firewall.

Data security by design

Fail to plan, plan to fail: having the right policies and processes in place (in relation to third party administrators as well as the trustees) will help to prevent cyber breaches.

- Do you have documented policies covering data security, encryption etc?
- Do you scan all removable media (memory sticks etc) for malware before allowing data to be imported onto your systems?
- Are your IT systems and processes kept up-to-date (eg applying updates and patches promptly)?
- How is data stored? Is it backed up securely?

Trustee protection

The best protection is training and proper processes, to make sure that everyone involved is vigilant about preventing cyber breaches, but in case the worst happens:

- Your contract with your administrators (or other processors) should include a clear allocation of cybersecurity risks and governance responsibilities, from minimum requirements, monitoring and reporting, to incident management, liability and compensation in the event of breach.
- Check whether your liability insurance covers cybersecurity-related acts or omissions and, if so, whether this also covers your delegates. Do you need a specific policy to cover cyber risk, and do your administrators and other providers carry insurance that covers these risks?
- Consider cyber response insurance that will help you in the immediate aftermath of a breach by identifying any weaknesses and making your data secure again. If you don't want to use insurance, do you have contact details of a company or expert that can help if the worst happens?

Member access

Encourage members to take the security of their pension information as seriously as that of bank accounts (eg using strong passwords that are not recorded with log-in details).

- If members have online access to personal accounts, are appropriate security measures in place (eg minimum password requirements and other identity checks)?
- Cyber-attacks often work by mimicry ('spoofing') – if an email looks genuine, the recipient may click on a malicious link within it, introducing malware into the system. Do members know how to verify whether communications that apparently come from the trustees are genuine?
- Use newsletters to encourage the use of strong passwords for scheme website/ member accounts and to provide instructions to help members protect themselves from spoofing. Encourage a pro-reporting culture to help you find out quickly about any attempts to infiltrate scheme systems.

Data retention and disposal

Some formal records and books have minimum legal retention periods attached, but trustee records may need to be kept for much longer periods in case of future queries or complaints about member benefits.

- Your record-keeping protocols should ensure that adequate information is kept centrally and securely on behalf of the scheme.
- Establish a policy for data retention and secure disposal in relation to trustees' personal file copies which include member data (for example, old emails or hard copies) and regularly ask trustees to confirm compliance.
- Obtain assurances from retiring trustees that all personal data obtained in connection with their trusteeship has been deleted or securely destroyed.

For more information on avoiding and managing pensions disputes, please visit our Pensions in Dispute site at **www.allenovery.com/pensionsindispute**

Key contacts

Maria Stimpson
Partner
+44 20 3088 3665
maria.stimpson@allenovery.com

Däna Burstow
Partner
+44 20 3088 3644
dana.burstow@allenovery.com

Neil Bowden
Partner
+44 20 3088 3431
neil.bowden@allenovery.com

Jane Higgins
Partner
+44 20 3088 3161
jane.higgins@allenovery.com

Jessica Kerslake
PSL Counsel
+44 20 3088 4710
jessica.kerslake@allenovery.com

Jason Shaw
Senior Associate
+44 20 3088 2241
jason.shaw@allenovery.com

Andrew Cork
Senior Associate
+44 20 3088 4623
andy.cork@allenovery.com

Helen Powell
PSL Counsel
+44 203 088 4827
helen.powell@allenovery.com