Industry Update

Protecting scheme and members' data from hacking and other cyber risks

The Pensions Regulator has made it clear that Scheme Trustees are responsible for the security of all data within a pension scheme and all of its records in whatever format, electronic or otherwise.

Scheme and members' data, including such information as N.I. numbers, salaries, dates of birth and bank account particulars can be invaluable to criminals and therefore such information should be protected.

Although holding considerable financial assets, pension schemes seldom employ the same degree of security systems, safeguards and protocols used by other financial institutions.

What are the specific risks?

Aside from physical office security such as locked premises and storage and the restriction of unauthorised persons from sensitive office areas, other data security risks can be posed by:

- emails (containing sensitive data) being sent to the wrong recipient or being requested by a fraudulent third party;
- computer data being stolen, destroyed or corrupted by malicious software, viruses or bugs;
- loss of PC hardware such as laptops being used at home by employees;
- hacking into the computer systems used by the Trustees, administrators or other associated parties.

What could result from these risks?

If any part of the scheme's or members' data is fraudulently accessed by any third party, whether maliciously or for criminal gain, the consequences could include:

- a breach of the data protection laws by Trustees, individually or collectively;
- loss of member confidence in the scheme and all of those associated with it;
- regulatory penalties; and
- time/cost implications in dealing with the fallout of the initial breach of trust and its subsequent consequences.

How can this risk area be minimised?

As part of the Trustees' regular governance processes, it must be ensured that periodic reviews of the security of the scheme's data is undertaken.

This will include:

1. Security reviews of the IT systems used by the Trustees and employer to ensure adequate attention to data communication, storage, disposal, and the security and integrity of those people with access to such systems. This may include the use of encrypted communication of scheme and member data.

2. Checking that similar security levels are applied to all other forms of communication, e.g. telephone calls and correspondence to members and other interested parties.

3. Requesting assurance from all administrators and other parties associated with the scheme to ensure that all recognised industry standards with regard to scheme data security are adhered to.

4. Having in place a contingency plan to deal with any outcome not already considered.

5. Providing adequate training and monitoring of all employees handling sensitive scheme data, including instruction of how to deal with any situation that may present a potential risk to the Trustees, the scheme, its members or the employer.

Finally, any Trustees not confident in the issues outlined in this document should seek professional guidance.

If you would like to discuss this further, please get in touch with your usual contact at Cartwright.

January 2017

Mill Pool House
Mill Lane
Godalming
Surrey GU7 1EY

T: 01483 860201

E: enquiries@cartwright.co.uk

250 Fowler Avenue
Farnborough Business Park
Farnborough
Hampshire GU14 7JP

T: 01252 894883

E: enquiries@cartwright.co.uk

Marlborough House
Victoria Road South
Chelmsford
Essex CM1 1LN

T: 01245 293300

E: enquiries@cartwright.co.uk

The Mansley Business Centre
Timothys Bridge Road
Stratford Enterprise Park
Stratford-upon-Avon
CV37 9NQ

T: 01245 293300

E: enquiries@cartwright.co.uk