Cyber resilience – are you ready?

Cybercrime remains one of the most rapidly evolving, yet poorly understood risk topics. Whilst the consequences of a cyber-attack on a company are well known, for pension schemes cyber risks are a relatively new threat.

In this emerging area, there are many potential actions that scheme managers, administrators and their suppliers can take to ensure that they are prepared for the possibility of a cyber-attack.

Why is this important?

Pension schemes hold an abundance of member data and assets making them very attractive targets for hackers. An attack could lead to identify theft of its members, financial losses, disruption of services and reputational damage to both the scheme and FRA/administrator.

What does this mean for scheme managers?

The initial starting point is asking a lot of questions and establishing an action plan. Scheme managers, with the support of their administrators and advisers, should attempt to understand what risks they could face and consider potential vulnerabilities within their set up before embarking on a plan to minimise those risks, where possible.

In particular, questions should be posed to:

- Data handlers/processors (such as administrators or payroll providers)
- Software suppliers
- The Fire and Rescue Authority (FRA) and any in-house teams.

What should scheme managers do?

Scheme managers should carry out a robust assessment of their FRA in order to take a holistic and structured view of the issue.

Aon's Cyber Solutions combine three critical areas to help our clients to understand and manage the minefield of cyber security.

Seek

- **Assess** – Identifying critical assets that could be at risk – what could go wrong?
- **Quantify** – Understanding the potential impacts of cyber threats were they to materialise is important.
- **Test** – A clear understanding of what controls are in place by all third parties and internal functions to prevent cyber-attacks.

Shield

- **Improve** – Improvements may need to be made to security systems.
- **Transfer** – Considering whether the exposed risk can be transferred to someone else.

Solve

- **Respond** – Ensuring that a plan is in place to tackle any incident should the worst happen.

Actions

As cybercrime is an evolving risk, it's critical that the risk is managed and as a minimum, we recommend the following:

- Obtain some training and discuss the issue with relevant parties.
- Undertake a robust assessment to identify specific risks and actions and document these on your risk register.
- Take forward any practical actions.

Risk. Reinsurance. Human Resources.
25 Marsh Street | Bristol | BS1 4AQ
t +44 (0) 117 929 4001 | f +44 (0) 117 925 0188 | aon.com

Empower Results®