

Pension Scheme Cyber Resilience Workshop



Cyber Resilience Workshop

Pension schemes hold substantial amounts of personal data, have regular financial transactions, and are managed by trustees who often have no dedicated IT support. As such they are prime targets for a cyber-attack. Aon's cyber resilience workshop will help trustees establish their key risks and come up with a plan to protect their scheme's data, assets, members and sponsor, as well as themselves.

Schemes at risk

Pension schemes in the UK hold millions of member records and have billions of pounds in assets. Both move around regularly. This makes them a prime target for cyber-attacks.

Pension schemes, sponsors and regulators have now woken up to this threat, and most schemes are considering how they deal with cyber risk alongside the range of other risks that they face.

The challenge for trustees is that this is a new area for them, the risks are constantly evolving and the actions are not immediately obvious.

Where to start

With so many moving parts in a pension scheme, depending on who trustees speak to, different actions may be recommended. It is hard to know where to start:

- Penetration testing of adviser systems
- Questionnaires to understand adviser controls
- Security of trustees working on personal devices, or using personal emails
- Insurance protections
- Incident response planning

In practice, the place to start depends on the circumstances of the scheme and sponsor, as well as factors such as previous experience and actions already taken in this area.

The danger of leaping straight into actions is that there may be bigger priorities that have not been considered, or quick wins that can have an immediate impact.



Planning a workshop

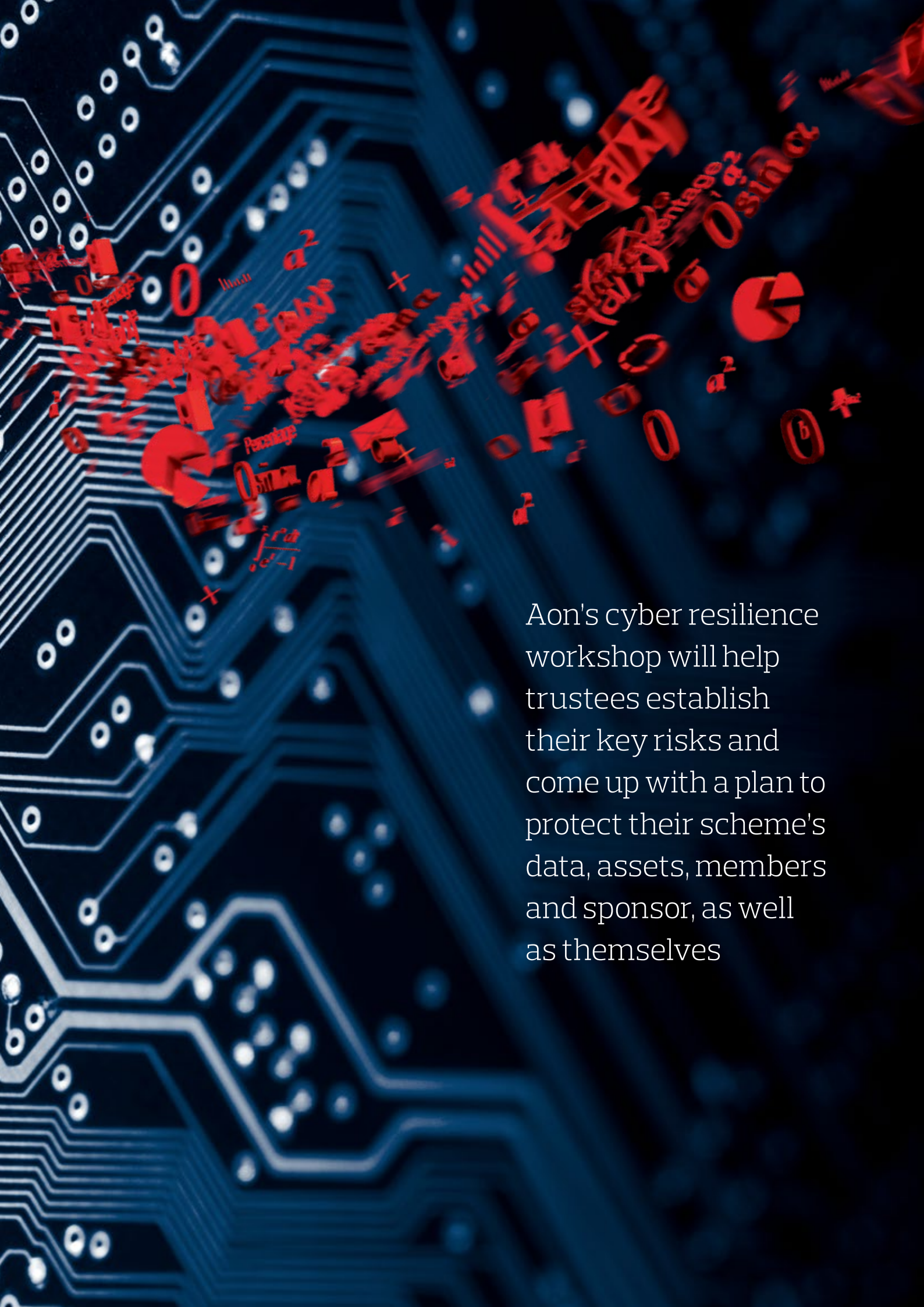
Aon's recommended approach to cyber risk is that trustees initially run a cyber resilience workshop, to identify the scheme's key threats and practical actions. These workshops are particularly valuable when opened up to include the sponsor, the IT department and trustees' advisers.

The purpose of the workshop will be to contribute towards the following actions:

- **Identify the context**
Determine scheme critical information and assets (ie hardware, software, data and scheme assets); who has access to these, and how information is relayed between different providers to create a network mapping (this may overlap with GDPR work).
- **Evaluate cyber resilience**
Evaluate performance of current controls to manage cyber threats, prioritise risks and improvement opportunities, including understanding current level of insurance and opportunities to transfer any residual risks.
- **Define the threat profile**
Identify threats facing the scheme, liaising with service providers and the sponsor to understand their cyber security processes and identifying any potential weaknesses.
- **Define incident response plan**
Support the development of an appropriate incident response protocol and framework.

The outputs from the exercise will identify opportunities for enhancing the risk management framework and recommend areas for further analysis and risk improvement.

More details on the workshop are shown on the next page



Aon's cyber resilience workshop will help trustees establish their key risks and come up with a plan to protect their scheme's data, assets, members and sponsor, as well as themselves

Workshop structure

Although the pension scheme is the responsibility of the trustee board, the stakeholders and those involved in the scheme are extensive, including the trustees, the members, the employer and a range of advisers. Rather than approach all of these stakeholders individually, an effective way to initiate a cyber risk project is to run a workshop with as many of the relevant people as possible, to understand the existing situation and where the key risks are likely to be. This can be done with one of our cyber specialists and an Aon retirement adviser who specialises in cyber for pension schemes, with the aim being to help establish clear objectives for the project.

The format of a typical workshop is as follows:

Pre-workshop

Prior to the workshop, we will obtain high level details of the scheme and how it operates in order to tailor the workshop to meet your circumstances. We also ask the attendees to do some pre-work, in particular for any third party or company representative to be aware of the following types of information:

- Knowledge of the cyber security policies, staff training and verification of individuals and/or instructions when transferring funds or providing member specific information.
- The level of insurance protection offered to the schemes and the trustees.
- How trustees are advised of any cyber incidents at a third party and, at a high level, knowledge of incident response plans.

Workshop

The workshop will typically last three hours and would take the following format:

- Overview of the cyber landscape and how this then translates into the pension scheme environment.
- Breaking out into groups and identifying how the trustees and other stakeholders are equipped to deal with specific scenarios.
- Discussion on the issues raised in the role play; this will be centred around the themes from the Aon Cyber Resilience Solutions Framework.
- Agreeing the next steps and specific actions.

For some schemes, we have extended the workshop to cater for the sponsor to present a short session on their cyber position or any incidents which may have impacted their operations. We can accommodate any additional items into the workshop to ensure that all attendees get the most out of the day.



Post-workshop

The output from the workshop will be written up in a summary setting out the initial findings and an action plan.

We envisage that the action plan may include steps to further investigate a range of areas, such as:

- Intricacies of the network mapping
- Current insurance provisions
- Cyber and data security policies and processes by all stakeholders
- Incident response planning

Robust framework

At the heart of our workshops is the Aon Cyber Resilience Framework (ACRF). The ACRF has been developed over many years by Aon working in conjunction with corporate clients and insurers, tackling cyber risk in businesses around the globe.

It is a tried and tested approach which ensures that all relevant aspects of cyber risk are considered, in a rigorous fashion, rather than diving into one specific area and risk missing a key issue.

Although developed for use with corporate clients, it is equally applicable to pension schemes, and our workshops use a version that is adapted specifically for pension schemes.

Aon Cyber Resilience Framework (ACRF)



Identify critical assets, vulnerabilities and risks, to assess organisational preparedness



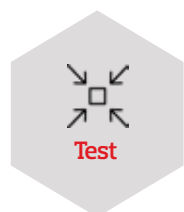
- Member data
- Financial transactions
- The reputation of the sponsor
- In-house administration or payroll
- Data mapping and GDPR

Quantify the financial impact from cyber risk to inform risk reduction and transfer strategies



- Financial impact
- Reputational impact
- Operational impact

Uncover, test and remediate application, network and endpoint vulnerabilities



- Suppliers' systems
- Sponsor's systems
- Physical security
- Trustees' own arrangements
- Staff training as well as IT

Prepare, optimise and enhance security, governance, incidence detection and protocols



- Existing mitigations
- Future mitigations
- Prioritisation
- Risk register
- Monitoring

Explore risk transfer solutions to minimise balance sheet risk



- Indemnification and exoneration
- Trustee liability insurance
- Cyber policies or extensions
- Contracts
- Policy wording and exemptions

Limit business disruption, minimise economic loss and expedite the claims management process



- Incident response plan
- Critical contact details
- Rapid response support

Contacts

Vanessa Jaeger
Principal Consultant
+44 (0)1727 888230
vanessa.jaeger@aon.com

Paul McGlone
Partner
+44 (0)1727 888613
paul.mcglone@aon.com

Emma Moore
Senior Consultant
+44 (0)1179 004496
emma.moore@aon.com

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

For further information on our capabilities and to learn how we empower results for clients, please visit <http://aon.mediaroom.com>.

This document and any enclosures or attachments are prepared on the understanding that it is solely for the benefit of the addressee(s). Unless we provide express prior written consent, no part of this document should be reproduced, distributed or communicated to anyone else and, in providing this document, we do not accept or assume any responsibility for any other purpose or to anyone other than the addressee(s) of this document.

Notwithstanding the level of skill and care used in conducting due diligence into any organisation that is the subject of a rating in this document, it is not always possible to detect the negligence, fraud, or other misconduct of the organisation being assessed or any weaknesses in that organisation's systems and controls or operations.

This document and any due diligence conducted is based upon information available to us at the date of this document and takes no account of subsequent developments. In preparing this document we may have relied upon data supplied to us by third parties (including those that are the subject of due diligence) and therefore no warranty or guarantee of accuracy or completeness is provided. We cannot be held accountable for any error, omission or misrepresentation of any data provided to us by third parties (including those that are the subject of due diligence).

This document is not intended by us to form a basis of any decision by any third party to do or omit to do anything.

Any opinions or assumptions in this document have been derived by us through a blend of economic theory, historical analysis and/or other sources. Any opinion or assumption may contain elements of subjective judgement and are not intended to imply, nor should be interpreted as conveying, any form of guarantee or assurance by us of any future performance. Views are derived from our research process and it should be noted in particular that we can not research legal, regulatory, administrative or accounting procedures and accordingly make no warranty and accept no responsibility for consequences arising from relying on this document in this regard.

Calculations may be derived from our proprietary models in use at that time. Models may be based on historical analysis of data and other methodologies and we may have incorporated their subjective judgement to complement such data as is available. It should be noted that models may change over time and they should not be relied upon to capture future uncertainty or events.

To protect the confidential and proprietary information included in this material, it may not be disclosed or provided to any third parties without the prior written consent of Aon.

Aon does not accept or assume any responsibility for any consequences arising from any person, other than the intended recipient, using or relying on this material.

Copyright © 2020. Aon Solutions UK Limited. All rights reserved.

Aon Solutions UK Limited Registered in England and Wales No. 4396810 Registered office:
The Aon Centre, 122 Leadenhall Street, London, EC3V 4AN.

Aon Solutions UK Limited is authorised and regulated by the Financial Conduct Authority.

Aon Solutions UK Limited's Delegated Consulting Services (DCS) in the UK are managed by Aon Investments Limited, a wholly owned subsidiary, which is authorised and regulated by the Financial Conduct Authority.

www.aon.com