



Pensions Cyber Risk

Pulling it all together

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.

Over recent years pension schemes have stepped up how they manage cyber risk, but for many schemes this is still somewhat ad-hoc. With greater emphasis being placed on internal controls, managing cyber resilience through a series of regular tasks is the next step.


Importance of managing cyber risks

Cyber risk has been an increasingly topical issue for pension schemes. As cyber risk management requirements for pension schemes matures, so does the approach that needs to be taken.

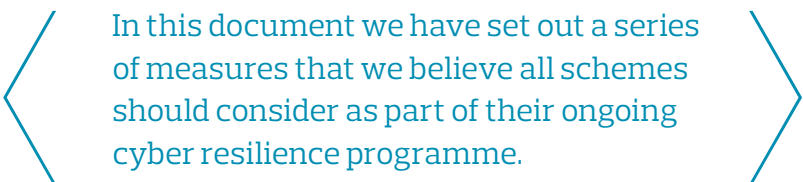
The Pensions Regulator released guidance back in April 2018 on the issues it expects trustees and scheme managers to consider in order to increase their cyber resilience. While many schemes have already taken some action, those actions are often taken in isolation with no longer term plan.

For schemes to deal with cyber risk adequately, cyber risks need to sit alongside other scheme risks; with ongoing internal controls and other checks to ensure security of members' benefits along with scheme assets. This is particularly important given the pace at which cyber threats change.

As this is a relatively new area for trustees, the actions are not immediately obvious, and what "good" looks like is constantly evolving.



"The cyber risk paper was the best thing we have ever seen on cyber risk – so practical!"



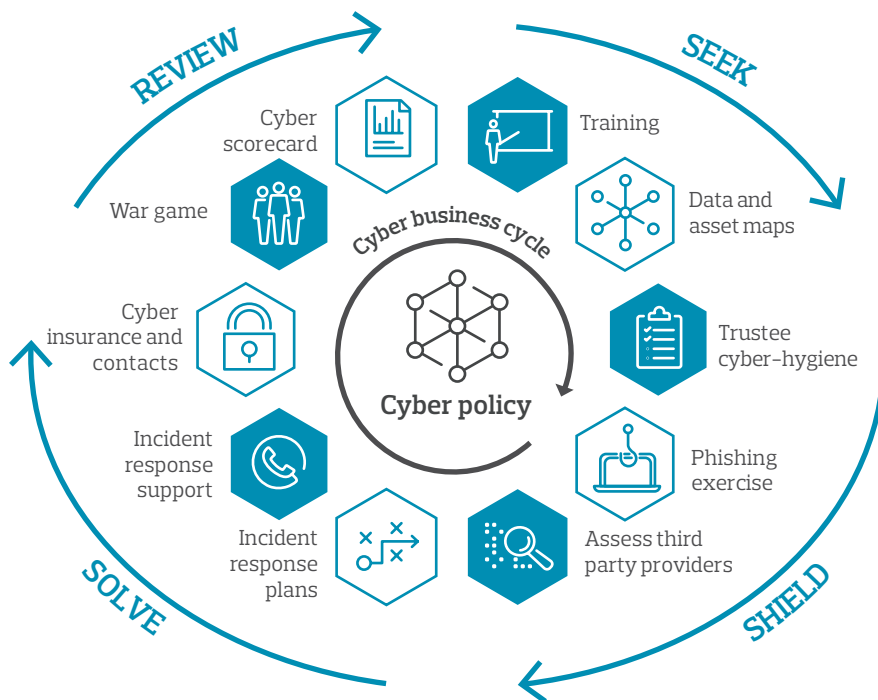
In this document we have set out a series of measures that we believe all schemes should consider as part of their ongoing cyber resilience programme.

Overall cyber strategy

Aon's Cyber Business Cycle for pension schemes sets out the key stages to improving your scheme's cyber resilience. The cycle follows a 'Seek', 'Shield', 'Solve' and 'Review' framework.

- **Seek** is about understanding your cyber risks, what you are exposed to
- **Shield** is about protection – actions that you can take to limit the chances of an incident
- **Solve** is about dealing with an incident should the worst happen
- **Review** is about recognising that cyber risk is not a static risk and therefore a framework for ongoing review should be established

Increasingly we are seeing more schemes document their cyber strategy as it helps ensure actions are prioritised in accordance to risk levels.



"The War Game was one the most worthwhile hours we have spent as Trustees."

With so many possible actions it is hard to know where to start. The Aon Cyber Scorecard provides an assessment of your current position and highlights opportunities for quick wins.

Once the initial assessment is done, many schemes start with either a War Game or Third Party Assessment, and quickly move onto an Incident Response Plan. But once the basics are in place that does not mean the job is done. These documents and processes will still need revisiting from time to time.

Aon recommend that schemes put in place a series of cyber-related actions which are revisited over a 2-year cycle. The precise details will vary from scheme to scheme.

More detail on the actions shown in the Cyber Business Cycle is set out on the following pages.

Cyber business cycle components

The needs of each pension scheme will differ, but common components of a cyber resilience framework will include the following:

Periodic training

Cyber risk is not something that most trustees come across in their day jobs, so periodic training is essential. This could be external events or scheduled at trustee meetings. Training could come from external cyber experts, internal resources or advisers and suppliers. Mixing up the training from year to year is helpful, and the focus needs to be on actions, not on just 'scaring' the trustees.

Data and asset maps

Capturing all the places that scheme data and/or assets are held, and how they move around is key to understanding the scope of cyber risk and where to prioritise actions. This can help inform where to focus third party assessments and the level of scrutiny involved in that assessment.

Trustee cyber-hygiene

Trustees can be the weakest link in a scheme's cyber footprint, with many using home email accounts and almost certainly not having the same level of security that advisers do. Many schemes have a document describing what the scheme expects of its trustees in relation to cyber security, which should be regularly reviewed.

Phishing exercise

Over 90% of cyber-attacks still start with a relatively basic phishing campaign. Most large organisations run fake phishing campaigns to test the resilience of their systems and the level of knowledge of their staff. Pension scheme trustee boards are not large enough to do this, but by bringing together multiple pension schemes Aon has run two industry exercises in recent years, covering over 600 trustees.

Third party assessments

A key part of a cyber strategy is to monitor the arrangements made at third party advisers and suppliers, including the sponsor if they provide any services to the scheme. Different levels of assessment will be appropriate for different providers.

Incident response plan (business continuity plan)

No business would dream of dealing with a major incident without an incident response plan, and increasingly trustees and their sponsors feel the same way about their pension schemes. While plans can never be overly detailed, they certainly can provide a good framework for handling any incident, including wider business continuity planning. Perhaps the most difficult issue is how the plans of the trustees, sponsor and advisers interact in practice.

Incident response support

One of the key learnings from simulated cyber-attacks (war games) is that cyber events can quickly become all-consuming, with the trustees dealing with the source of the problem, the sponsor, lawyers and other advisers, members, media, insurers etc. Coupled with unfamiliar content, the thought of handling an incident can be daunting. Having a cyber specialist on retainer means support for the scheme if an attack takes place.

Cyber insurance

Cyber insurance is a rapidly growing market. While many corporates now have some form of cyber cover, it does not normally extend to the pension scheme, and Trustee Liability Insurance only tends to cover claims against the trustees. Specialist pension scheme cyber insurance is slowly emerging as a new product.

War game

Running a simulation of a cyber-attack is one of the most effective ways of engaging the trustees, the sponsor and the advisers in a discussion of risks and actions. It can be used either as part of an initial training exercise, a half day workshop or to test incident response plans.

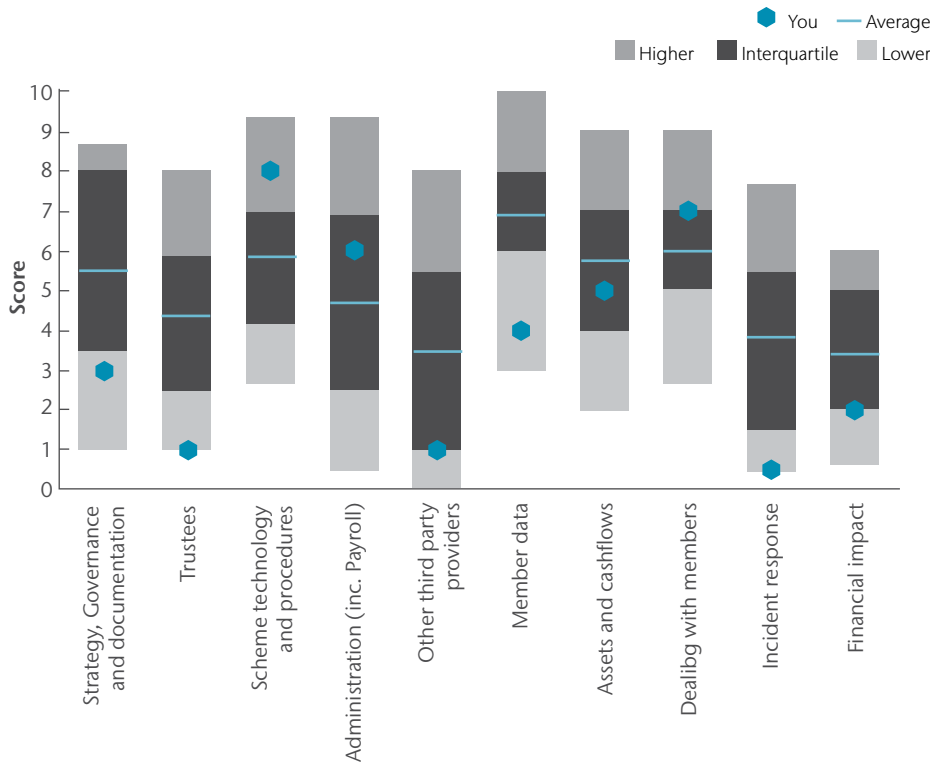
Cyber policy

Having an overall cyber policy allows trustees to document their risk management approach and priorities, as well as being something that can be shared with other interested parties and auditors.

Cyber Scorecard

Aon's Cyber Scorecard provides an assessment of your current position and highlights opportunities for quick wins. It is based on 50 multiple-choice questions that most trustees, pensions managers or scheme secretaries should be able to complete. It is free to all schemes and provides an assessment in ten key areas, including benchmarking against the market.

If you would like to find out more information on the cyber risk services and packages Aon provides then please contact a member of the Aon Pensions Cyber Risk team.



Contact information

Vanessa Jaeger
Principal Consultant
+44 (0)1727 888 230
vanessa.jaeger@aon.com

Paul McGlone
Partner
+44 (0)1727 888 613
paul.mcglone@aon.com

For your free cyber scorecard, visit www.aon.com/cyberscorecard

To see the results of the scorecard across the first 100 schemes that have completed it visit www.aon.com/unitedkingdom/retirement-investment/trustee-effectiveness/cyber-threats-to-corporate-pension-schemes.jsp

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 © 2021. 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.

