

Pensions: Cyber Risk in the Public Sector

Putting it all together

Scheme managers hold substantial amounts of member personal data, have regular financial transactions, using a variety of systems including in-house IT systems with the host authority, and often bespoke systems for the administration, investment and management of the Fund. Scheme managers also usually have data and assets that are held with external suppliers. As such they are prime targets for a cyber-attack.

Over recent years scheme managers have stepped up how they manage cyber risk, but given the range of service providers and fast paced nature of cyber security 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 all pension schemes including public sector schemes. As cyber risk management requirements for pension schemes matures, so does the approach that needs to be taken.

The Pensions Regulator released guidance 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. In recent years the Regulator has also asked a number of questions in their Public Service Pension Scheme Annual Survey on the topic of cyber resilience to assess progress being made by schemes.

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 scheme managers, the actions are not immediately obvious, and what "good" looks like is constantly evolving.

Cyber resilience components

Common components of a cyber resilience framework include the following:

Periodic training

Cyber risk isn't something that those involved with managing pension schemes may come across in their day jobs, so periodic training is essential. This could be external events or scheduled at senior management, pension committee and pension board 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" those responsible for managing the scheme.

Setting expectations

Representatives on pension committees and pension boards can be the weakest link in a scheme's cyber footprint, with some using home email accounts and almost certainly not having the same level of security that officers, elected members and advisers do.

Many schemes have a document describing what the scheme expects of those involved in the management of the scheme in relation to cyber security, which should be regularly reviewed.

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

Third Party assessments

The most essential part of a cyber strategy is to monitor the arrangements made at third party advisers and suppliers, including the host authority if they provide any services to the scheme manager and suppliers hosting IT systems. Different levels of assessment will be appropriate for different providers. For those with in-house arrangements, our CyQu tool is a great cost effective tool to assess any vulnerabilities. Our separate “Cyber Security Assessments” document provides more details.

Incident Response Plan

No business would dream of dealing with a major incident without an incident response plan, and increasingly scheme managers and their host authorities feel the same way. While plans can never be overly detailed, they certainly can provide a good framework for handling any incident. Perhaps the most difficult issue is how the plans of the scheme manager, host authority and advisers interact in practice.

War Game

Running a simulation of a cyber-attack is one of the most effective ways of engaging the pension committee, pension board and senior officers in a discussion of risks and actions. Involving the host authority and/or advisers can make it more meaningful where the exercise spans areas they are responsible for. It can be used either as part of an initial training exercise, a half day workshop or to test incident response plans. For more information see our separate documents entitled “Aon Cyber Attack Simulation Exercise (“War Game”)” and “Pension Scheme Cyber Resilience Workshop”.

Expert on Retainer

One of the key learnings from simulated cyber-attacks (war games) is that cyber events can quickly become all-consuming, with the scheme managers dealing with the source of the problem involving engagement with the host authority, 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 doesn't 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. Get in touch with us if you would like to know more about cyber insurance.

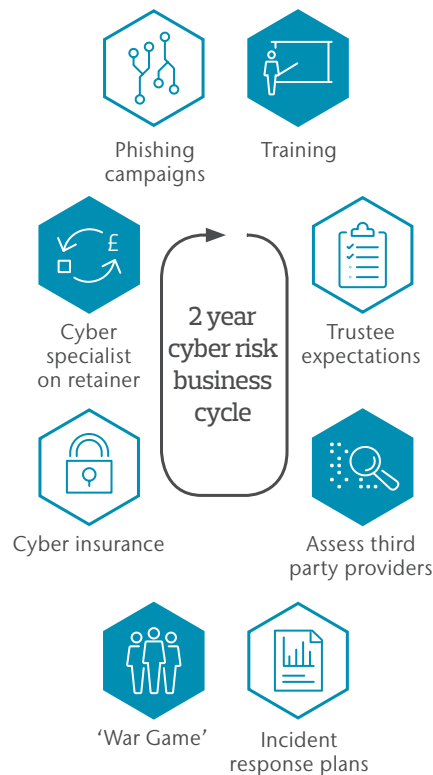
Phishing exercise

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 committees, boards and officer teams are often not large enough to do this, but by bringing together multiple pension schemes, or extending this to a larger host authority, Aon is able to offer such a service. Our document entitled “Trustee Phishing Exercise” contains more details.

A cyber risk business cycle

With so many possible actions it's hard to know where to start. Most 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 doesn't mean the job is done. These documents and processes will still need revisiting from time to time. Aon recommend that scheme managers put in place a series of cyber-related actions which are revisited over a two year cycle.

The precise details will vary, but a sample timeline is shown below:



Actions also need to link to other scheme governance such as the business plan, risk register and internal controls.

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 Public Sector team.

We're here to empower results

Karen McWilliam

Head of Public Sector Governance and Benefits Consultancy
+44 (0)7711 016 707
karen.mcwilliam@aon.com

Daniel Kanaris

Senior Benefits and Governance Consultant
+44 (0)117 900 4447
daniel.kanaris@aon.com

Catherine Pearce

Senior Benefits and Governance Consultant
+44 (0)117 901 3419
catherine.pearce@aon.com

Mary Lambe

Senior Benefits and Governance Consultant
+44 (0)1727 888 236
mary.lambe@aon.com

Craig Payne

Senior Benefits and Governance Consultant
+44 (0)117 945 3523
craig.payne@aon.com

Ben Challinor

Benefits and Governance Consultant
+44 (0)121 335 3720
ben.challinor@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/>

© Aon plc 2020. All rights reserved.

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Aon Hewitt Limited is authorised and regulated by the Financial Conduct Authority. Registered in England & Wales. Registered No: 4396810.