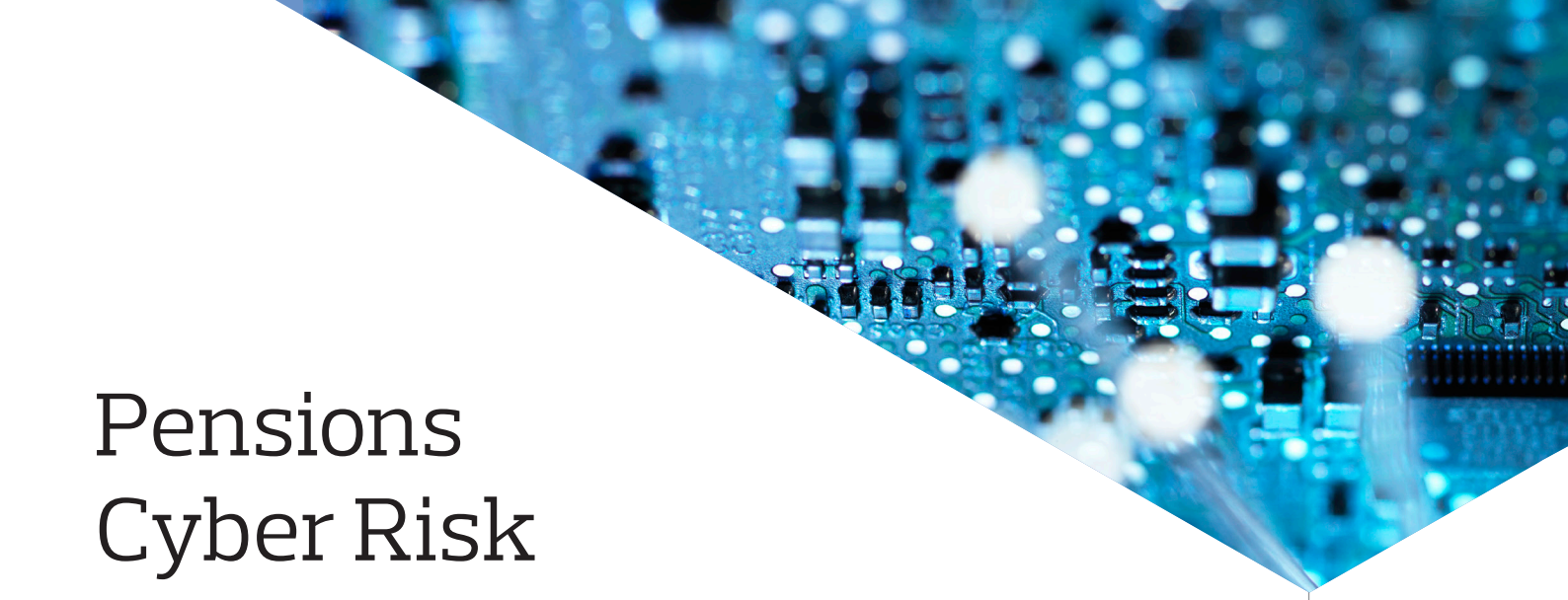


Pensions Cyber Risk

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.

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

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 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.

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.

AON
Empower Results®

Cyber resilience 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 isn't 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.

Trustee expectations

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.

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 sponsor if they provide any services to the scheme. Different levels of assessment will be appropriate for different providers. 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 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. Perhaps the most difficult issue is how the plans of the trustees, sponsor and advisers interact in practice.

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. 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 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 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 scheme trustee boards are not large enough to do this, but by bringing together multiple pension schemes Aon is able to offer such a service. Our document entitled *"Trustee Phishing Exercise"* contains more details.

Aon's cyber resilience framework ensures that all aspects of cyber risk are considered

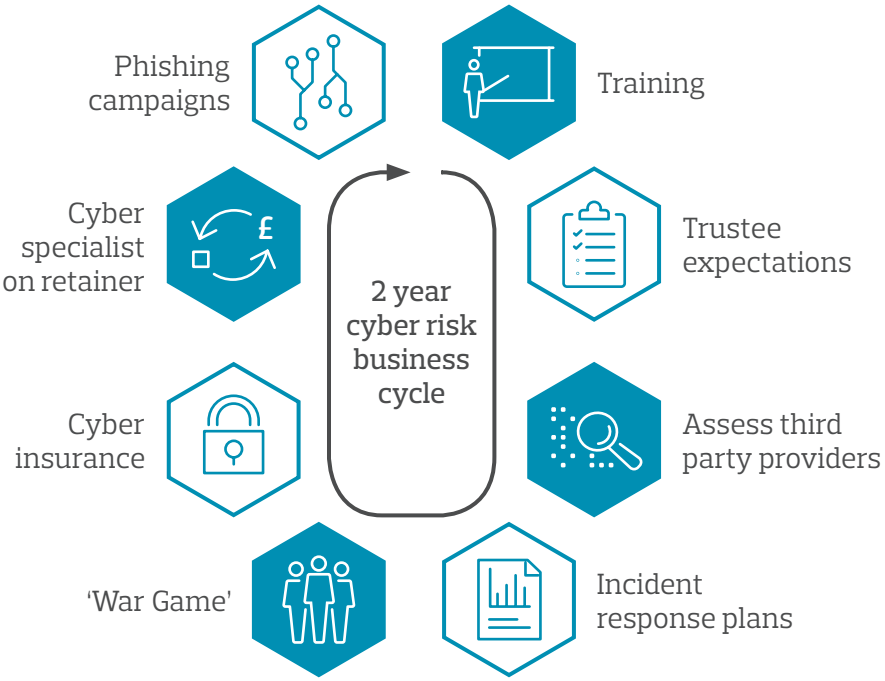
A cyber risk business cycle

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 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, 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 Pensions Cyber Risk team (see contact information).



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

Emma Moore
Senior Consultant
+44 (0)1179 004 496
emma.moore@aon.com