Aon
Retirement and Investment

Aon Investment Research and Insights

How to Protect your Pension Scheme from Cyber Risks through Asset Managers

July 2018

Empower Results®

Table of contents

About Aon Investment Research and Insights

Aon's robust portfolio of ideas, tools and researched solutions supports trustees and sponsors to anticipate their future investment requirements.

By beginning to identify investment research and communicate ideas before they are needed we can shorten the implementation times for our clients and act in a timely way when opportunities are correctly priced.

To learn more and to access other research and insights from Aon's investment experts, visit **aon.com/investmentuk**

Introduction

Over the past 12 months, cyber risk has leapt up the agenda of pension schemes and sponsors, and is one of the most rapidly evolving issues that schemes face. With large volumes of personal and financial data processed within a relatively less sophisticated security environment, in comparison to other financial institutions, it is only a matter of time before pension schemes start to attract more explicit attention from cyber criminals.

But what should trustees and sponsors be doing about these risks? The good news is that, unlike many other pension issues, cyber risk is an area where there is extensive relevant corporate experience to draw upon, and considering how other organisations deal with this risk gives a strong framework for pension schemes to do the same.

In April 2018, The Pensions Regulator published their guidance on Cyber Security Principles for pension schemes, with a strong steer for trustees to understand their risks and put controls in place. Much of that guidance relates to dealing with member data, and the recent focus on the General Data Protection Regulations (GDPR) has also strengthened procedures to protect such data.

In this note, we focus on the cyber risks associated with assets, and specifically those which pension schemes are exposed to by using asset managers. In particular, we look at:

- The steps taken to mitigate this risk and
- Actions for trustee consideration

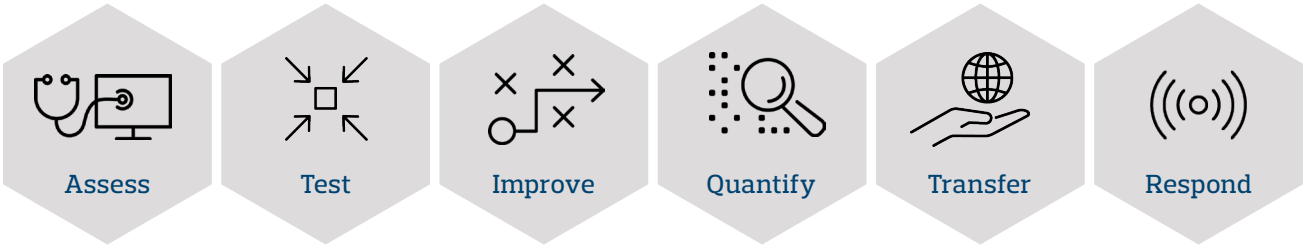
Issues for trustees to consider

Trustees should be aware of the cyber threats which they are exposed to through their assets managers and, if appropriate, explore how these risks could be reduced. We suggest that this evaluation should be carried out in conjunction with an overall review on cyber security within the pension scheme and documented in their risk register.

For trustees the key actions relating to pension scheme assets are to:

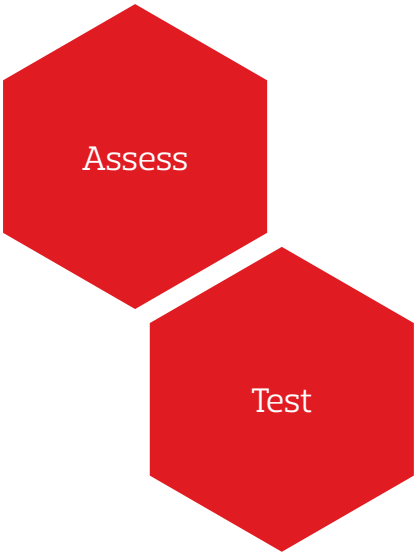
- Understand what protections are in place, both now and at regular points in the future;
- Understand how they will be notified of any breach, impacting their pension scheme assets;
- Understand if they are exposed to any residual risks, and to take action to mitigate these if required (and possible);
- Put in place a procedure to be notified of any breach, impacting their pension scheme assets.

Cyber resilience framework



Assess	Test	Improve	Quantify	Transfer	Respond
Identify critical assets, pinpoint vulnerablities and access cyber preparedness to improve risk exposure	Uncover, test and remediate application, network and endpoint vulnerabilities	Prepare, optimise and enhance security governance and incident detection and protocols	Model potential loss, mass exposure and remediation costs to optimise risk mitigation strategy	Risk transfer solutions to minimise balance sheet risk	Limit business disruption, minimise economic loss and expediate the claims management process

CYBER JOURNEY



Awareness of the approach taken by managers to reduce the risks

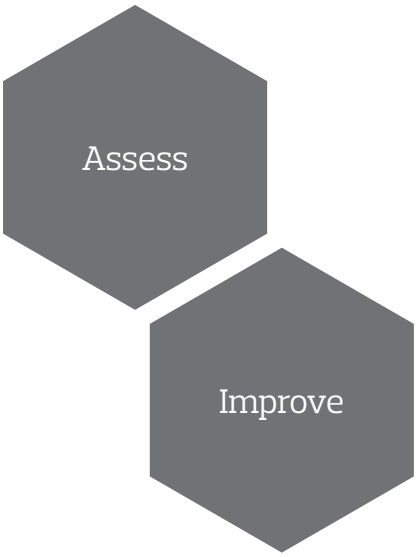
A key role for Aon as an investment consultant is to keep managers under review. While investment capability and potential performance is an important element, equally important are the processes in place to protect pension scheme assets.

We refresh our manager ratings on an ongoing basis, including periodic reviews that include an assessment of the manager's cyber security. The outcome of these reviews is communicated to clients alongside other aspects of our review, usually through their regular quarterly reports or through our InTotals.

Trustees are reliant on managers (and their third parties) to have robust processes and security to combat cyber risks. Trustees may want to review their contracts with their asset managers in order to understand what protections are offered if the asset manager were to be the target of a successful cyber attack. The trustees should then be able to identify the potential consequences in the event of a failure.

Awareness of the manager's incident response plans

As well as understanding the protections that are in place, trustees should understand what their asset manager(s) protocol is for advising of any cyber incident. In particular, when would they be advised of the incident and how will they be advised on any updates. This can then be incorporated into their own incident response plan.



Awareness of how the trustees themselves can mitigate cyber risks

Asset managers have control of the assets and so the primary cyber risks rests with them. However, another set of risks exists when investing and disinvesting monies. Usually trustees are authorised signatories but, if the trustees can be impersonated, then monies could be stolen. Trustees should:

- Know who are the authorised signatories who can invest and disinvest monies;
- Take steps to protect their identity;
- Inform the investment managers if they believe that they have been the victim of identity theft;
- Know which bank accounts pension scheme monies can be transferred to; and
- When sending signed instructions, take steps to protect their electronic signature e.g. by sending via encrypted emails/attachments.

Manager cyber risks

Most asset managers employed by Defined Benefit (DB) pension schemes do not hold member data. Therefore the type of cyber threats involving theft of member data is less of a concern.

However this may not be the case with managers of AVC and Defined Contribution (DC) assets. But irrespective of whether the pension scheme is DB or DC, asset managers may be exposed to the following forms of cyber risks:

Risk area	Potential method	Explanation
Fraud and identity theft (Theft of trustee details or manager's employee details)	Social engineering and phishing (the attempt to acquire sensitive information such as usernames and passwords)	Managers have to go through a process of verifying trustee details – this can involve passports, utility bills and other personal data, which can be stolen either directly from a system or via social engineering. It is important that this data is kept secure and up to date. Managers need to have the appropriate protocols in place to be able to identify the real instruction from a fraudulent attempt to access pension scheme funds.
Denial-of-service attacks	Computer viruses, Malware (malicious code), Ransomware and spam	The key risk here is that trades cannot be placed if the manager needs to change the portfolio to react to market events or invest/disinvest cash. It is important that managers have incident response plans in place to promptly and securely restore systems. A trustee incident response plan should consider what happens if investment/disinvestment is not available for some time.
Theft of proprietary information (Regarding investment process, portfolio holdings or trading information)	Eavesdropping, spoofing (communication is sent from an unknown source disguised as a source known to the receiver)	There would be a niche market to sell this type of data, for example potentially a competitor. Most people would not understand the information stolen or how to exploit it. However, managers will want to ensure that their Intellectual Property is not compromised. In practice this may be more of a concern to the manager than the trustees.
Theft of assets	Spoofing, tampering, clickjacking or social engineering	This involves either the electronic transfer of securities or cash or obtaining the details required to transfer securities or cash by false means. Again, managers need to have the appropriate protocols in place to be able to identify the real instruction from a fraudulent attempt to access pension scheme's funds.
Altering or deleting data	Any of the above	This is either done for amusement or to conceal a crime. Managers need to have the systems in place to identify a loss or change of data and an appropriate recovery method.

Manager controls

Investment managers have a range of measures to guard against these cyber threats.

These measures fall broadly into three categories:

1. Preventative measures to stop cyber attacks before they happen. Attacks are either deliberate, targeting a particular entity for something that has value, or opportunistic, when a scan reveals an exploitable opportunity. Cyber threats are prevented by examining people, processes and technology and looking to mitigate the impact of vulnerabilities arising from these three areas.

   Preventative measures include:

   Vulnerability assessment
   This is a risk-based approach to evaluating cyber threats such as assessing security structures, governance, operations, and controls, as well as considering specific threats relevant to their circumstances.

   Behavioural software
   An increasing number of managers use AI software that learns what is normal and then identifies unusual patterns in their network activity, thus identifying potential security threats. Darktrace is an example of one of the larger providers.

   Awareness training for staff
   Managers train their staff to recognise phishing emails and be aware of clickjacking (where a link is sent in an email). Managers frequently send their own phishing emails to staff to test their internal defences. Any employee who fails the test is then sent for further training.

2. Reactive measures incorporated into processes to identify, escalate, report, and mitigate the impact of a successful attack. However, if an attack cannot be quickly identified, then these measures may be worthless.

3. Checks on managers' third party providers such as custodians, banks and administrators to ensure that their controls are adequate.

Aon's approach to researching manager's cyber security

When researching new products and formulating a rating, we ask the managers to complete an Operational Due Diligence (ODD) questionnaire. The questionnaire is dynamic and is updated periodically to capture changes in the marketplace, evolving best practice, or specific rules and regulations such as the General Data Protection Regulations (GDPR).

The questionnaire is completed before we rate a product and from time to time thereafter. If the manager has other products which we want to rate, they have to complete the questionnaire again.

We also complete follow ups with the investment manager, often including a site visit, where we question the managers on any areas and gain an understanding of the areas that they feel are of most concern to them.

The ODD team have the ability to veto a rating, no matter how good the potential investment. It is very common for them to require improvements to processes before we rate a product.

Preventative measures

When Aon performs due diligence on managers, we like to see evidence of regular testing as well as rotation of the expert providers who carry out the testing. We also ask to see their vulnerability assessment and steps that they have taken to address any weaknesses identified. There are a series of best practice steps that are increasingly becoming market standard.

Insider risk is real so we also consider possible employee motivations (a poor appraisal, poor people management or an employee's financial situation) and ask questions to senior management teams on their protocols for detection of such issues.

In terms of security, we like to see access to IT systems limited to the employees who need it. We identify whether physical security measures are employed, such as locks on the server room door and making sure that USB ports on computers cannot be used. We also ask about the movement of staff, visitors and contractors within the premises.

Reactive measures

We expect managers to have a cyber incident response plan in place and to see evidence that the plan is regularly tested along with any improvements to the plan over time. We ask for details of the identification and response to incidents. In addition, we expect a business continuity plan to be in place as well as a disaster recovery plan and an effective crisis management framework.

We would also expect to see insurance in place to provide some level of compensation in the event of a loss arising from a cyber attack.

Third parties – administrators, custodians and banks

As part of Aon's due diligence, we check cash controls of managers and check that there are logical controls in the banking software between the manager and a third party administrator.

This means that a cyber attack has to breach two networks, rather than one, in order to move assets. It also means that the single point of failure is the bank rather than the manager or the administrator; banks are generally better-resourced to be able to respond to and recover from a situation where cash has been moved outside of established parameters.

Other actions for trustees

Whilst this note focuses on cyber risks introduced by using asset managers, there are many other aspects of pension scheme management that could be at risk from cyber threats. In our view, it is important that trustees undertake training to understand the range of potential cyber threats in order to determine which ones pose the greatest concern to them; be that loss of member data, denial of service of one of their providers or an attack leading to the inability to pay their pensioners one month.

Although The Pensions Regulator's guidance leans towards trustees turning into cyber experts, there are a number of straightforward practical actions that can be implemented.

For example,

- Establishing a trustee security policy setting out how trustees plan to keep confidential information (relating to assets, trustee identity and member data) secure,
- Reviewing and improving how information is transferred between all parties,
- Establishing and testing incident response plans.

Trustees may also want to undertake a review of protections offered to the pension scheme, looking at contracts, employer indemnities as well as insurance provisions. We have pension schemes now looking to take out cyber insurance.

Summary

Cyber threats are continually evolving, which requires potential targets to be continually reviewing their cyber security processes.

Cyber security is a necessary activity for asset managers. They and their suppliers are used to operating in a complex regulatory framework which requires many processes and procedures. This, together with the erosion of trust and reputational risk of a cyber breach, requires the development of their cyber security capabilities.

Aon's ODD process helps to ensure that the managers with the weakest cyber security are screened out before being put in front of our clients.

Nonetheless trustees should:

- Be aware what their managers are doing.
- Take measures to protect confidential information (asset details, trustee identity, member data).
- Understand what protections are in place by all of their providers, not just asset managers .
- Understand which residual risks exist and consider mitigation.
- Prepare and test their incident response plan, and know their providers' plans.

Aon can:

- Advise trustees on the outcome of our due diligence, including any concerns raised at regular manager reviews.
- Support the trustees with establishing an incident response plan and a trustee security policy which can cover the cyber risks of the pension scheme as a whole, not just those linked to asset management.
- Assist with helping trustees understand any residual risks, and advise trustees on any actions which may be taken to mitigate these, where possible.

Aon has extensive experience of supporting corporates with mitigating cyber risks and we have translated this experience into supporting sponsors and trustees of pension schemes of all sizes with tackling these issues.

For example, we have run a number of workshops with trustee boards to provide both education on mitigating cyber risks, as well as running table top exercises for incident response planning.

If trustees have not yet tested their GDPR data breach response plan, this could be a really useful exercise.

We're here to empower results

For more information visit
aon.com/investment
or contact your Aon representative.

Contacts

John Belgrove
Senior Partner
john.belgrove@aon.com
+44 (0)20 7086 9021

Kate Charsley
Partner
kate.charsley@aon.com
+44 (0)117 900 4414

Sion Cole
Senior Partner and Head of European Distribution
Delegated Consulting Services
sion.cole.2@aon.com
+44 (0)20 7086 9432
Follow me on twitter – @PensionsSion

Tim Giles
Head of UK Investment Consulting
tim.giles@aon.com
+44 (0)20 7086 9115

With thanks to our authors

Vanessa Jaeger
Principal Consultant

Rupert Kotowski
Principal Consultant

Lucinda Downing
Asset Allocation

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.com

Empower Results®