Lancashire Local Pension Board
Meeting to be held on Tuesday, 24 January 2023

Electoral Division affected:
N/A;

Annual Report on Cyber Security
(Appendix 'A' refers)

Contact for further information:
Catherine Hunt, , Senior Governance Officer, 01772 533757,
catherine.hunt2@lancashire.gov.uk

Executive Summary

To provide members of the Pension Board with a summarised position regarding Cyber Security for the Lancashire County Pension Fund.

Recommendation

The Board are asked to note the contents of the report.

Detail

The pensions team is required to provide an update on cyber security to the Lancashire Local Pension Board as part of the annual workplan. It is good practice to update the Pension Board on cyber security on a regular basis in line with the Pension Board's remit to ensure the effective governance and administration of the Pension Fund.

The Pensions Regulator considers cyber risk to be an area of high priority for pension scheme trustees, recommending that it is included on the Pension Fund risk register. The Pensions Regulator has produced guidance on, "Cyber Security Principles for Pension Schemes", which provides the necessary advice for oversight of this technical area. Furthermore, the Pensions Regulator has included cyber security as part of the Single Code of Practice, which will replace the current Code of Practice 14.

The Pensions Regulator broadly defines cyber risk as the risk of loss, disruption or damage to a scheme or its members because of the failure of its information technology systems and processes. It includes risks to information (data security) as well as assets, and both internal risks (e.g. from staff) and external risks (e.g. from hacking).

Lancashire County Pension Fund (LCPF) is accountable for large amounts of personal data and assets, which is held by various partners including:

- Local Pensions Partnership Administration Limited - member's personal data;
- Local Pensions Partnership Investments Limited - data on assets held by the Fund directly or via pooling;
- Lancashire County Council - financial information related to the Fund as well as members personal data; and
- Northern Trust – data on assets held by the Fund as well as financial transactions.
- Mercer- member's personal data and financial and other information relating to employers of the Fund

It was agreed at the Local Pension Board meeting in October 2021, to provide an annual report based on guidance provided by the Pension Regulator's Single Code of Practice. However, there have been delays in the Single Code of Practice which is now expected to be implemented in early 2023.

Compliance with the Single Code of Practice

The Single Code of Practice, (module 'ADM016- Cyber Controls'), is currently in draft format but very little is expected to change when the final version is published. The new code outlines the internal controls and measures that should be adopted to assess and manage cyber risk, and these can be found at **'Appendix A'**. As a starting point, the Fund officers have completed a Cyber Security Assessment produced by Aon to help assess the Fund's vulnerability and to check what controls are in place.

To further understand and provide assurance to the Fund regarding the controls they have in place, the following requirements of the draft Code have been considered when preparing a questionnaire for our providers.

- '*assess at appropriate intervals, the vulnerability to a cyber incident of the scheme's key functions, systems and assets (including data assets) and the vulnerability of service providers involved in the running of the scheme'*,
- '*ensure appropriate system controls are in place and are up to date e.g. firewalls, anti-virus and anti-malware products*'.

The Single Code of Practice only provides high level guidance on managing cyber risk and other publications within the industry have also been referenced to prepare the questionnaire such as –

- 'Pensions and Lifetime Savings Association's Made Simple Guide to Cyber Risk,
- Aon's Cybercrime checklist

Cyber Security Assessment

LCPF responded to a survey from Aon in August 2022 and were provided with a scorecard summarising the Fund's resilience across 10 areas.

The scorecard is a useful tool to support the Fund officers to identify and prioritise actions that can be taken to protect the Fund, the host authority and the participating employers and fund members. However, it has been identified that it will be useful to re-submit the survey responses based on further information obtained from partners to ensure that the Fund will focus on the most appropriate actions.

The pensions team have initially focused their attention on two areas including:

1. An assessment of our administration provider and obtaining assurance around their cyber resilience – this is a higher priority due to the volume of personal data handled by LPPA
2. An assessment of other third-party providers and obtaining assurance around their cyber resilience

Fund officers have issued a questionnaire to third-party providers and following receipt of responses, will most likely seek assurance from a cyber specialist, *'to satisfy themselves with service providers' controls'* - a requirement of the Single Code of Practice.

ISO27001 – Information Security Standard

ISO207001 is widely regarded as a standard for businesses to demonstrate to their stakeholders and customers that they are committed to managing information securely and safely. Organisations that have this standard can expect to benefit from the following: -

- Secure information in all forms, including paper-based, cloud-based and digital data
- Increased resilience to cyber-attacks
- A centrally managed framework that secures all information in one place
- Organization-wide protection, including against technology-based risks and other threats
- Be able to respond to evolving security threats
- Reduced costs and spending on ineffective defence technology
- Be able to protect the integrity, confidentiality, and availability of data

The Fund officers are encouraged that both LPPA and LPPI are accredited to the ISO27001 Information Security standard (including data protection and cyber resilience), and other providers are using the standard as a basis of their controls or in the process of adhering to the standard.

Risk Register

While some controls around Cyber Resilience are already outlined in 'O7-Information Security', this risk has been renamed to 'Cyber Resilience and Information Security' to ensure the importance of Cyber Resilience is adequately focused upon.

This supports compliance with the Single Code of Practice requirement to *'Ensure cyber risk is on the risk register and regularly reviewed.'*

Following receipt of responses to the questionnaire and receipt of a revised scorecard from Aon, the risk scores will be reviewed.

Going Forward

While there is still some activity required for the Fund to improve its cyber resilience, it is expected that the scorecard results will considerably improve following assessment and analysis of third-party providers. Early in the New Year Fund officers intend to resubmit answers to Aon for updated results, before prioritising future actions which will include but are not limited to the following: -

- Develop a Cyber Strategy outlining the Fund's plans on minimising cyber risk.
- Develop a Cyber Resilience Policy to define the Fund's expectations of our service providers and how and when compliance will be assessed
- Develop a Cyber Incident Response plan to enable the scheme to swiftly resume operations. This will include roles and responsibilities, escalation process, reporting of incidents and how critical functions will be maintained or restored
- Undertake a data mapping exercise to identify our data assets and flow of data so that exposure to risk is fully understood.
- Develop a Cyber Hygiene document outlining expectations of board and committee members e.g. regarding the use of computers and other devices and the retention and sharing of scheme data
- Undertake a financial impact risk assessment to evaluate the potential financial implications of a cyber threat
- Review contractual terms and conditions with partners to clarify any risks to the Fund

These actions will help improve the Fund's resilience and support compliance with the Single Code of Practice requirements.

The potential scope of cyber security work is significant and, at the point of drafting this paper, the pensions team is developing the strategic plan for the Pension Fund for 2023/24. As part of this, the scope of cyber security work will be defined and prioritised/costed against other projects.

Regular updates will be provided to the Board regarding the plan of activity and to provide further opportunity for engagement. A session regarding Cyber Security will also be included in the 2023/24 training plan.

Consultations

N/A

Implications:

This item has the following implications, as indicated:

Risk management

The threat of cyber-attacks is a growing, evolving and very real threat for all organisations. This poses a potential financial and reputational risk to the Fund. LCPF requires annual updates from their stakeholders to ensure that risks are being managed appropriately.

Local Government (Access to Information) Act 1985
List of Background Papers

Paper	Date	Contact/Tel

N/A

Reason for inclusion in Part II, if appropriate

N/A