Key decision: Not applicable
Unrestricted

Report to Pensions Committee

29 April 2022

Cyber Security

Report by Director of Finance and Support Services

Summary

The Pension Fund Risk Register has a red risk relating to cyber security. The paper below sets out some of the risks specific to the Pension Fund and how this risk is monitored and managed by the County Council, Hampshire Pension Services (as Administrators) and Link Fund Solutions (as Operator).

Recommendations

(1) Officers continue to monitor cyber security and risk

(2) Pension Committee Members and Pension Advisory Board members undertake to complete the LOLA training and the tPR toolkit training, as identified in paragraph 6.1.

Proposal

1 Background and context

1.1 The Pension Fund risk register currently has a red risk relating to cyber security and risk -

Cyber crime resulting in personal data for members being accessed fraudulently

1.2 Cyber risk can be broadly defined as the risk of loss, disruption or damage to a scheme or its members as a result of the failure of its information technology systems and processes. The risk has increased over the last year from amber to red to reflect the risk status on the Corporate Risk Register and the changing environment.

1.3 The Pension Fund relies on the WSCC corporate IT team to manage cyber security for information held on the corporate network and on Hampshire Pension Services for information held as part of the administration service provided. There is also a reliance on the cyber security measures in place with stakeholders and third-party providers including:

- Information received from over 200 participating employers
- Information received from over 80,000 members

- Information provided to EY as auditor
- Hymans Robertson as the Fund Actuary
- Link as investment manager for the Fund's liquid assets
- Northern Trust as custodian
- L&G as AVC providers
- Legal advisers, consultants and officers

1.4 The Pensions Regulator (TPR) has placed more importance on cyber security over the last few years and is interested in how pension schemes manage the risk. The Regulator does not expect LGPS schemes to only rely on Host Authority IT policies (i.e., WSCC) but to have their own assurance and mitigations in place. Cyber risk is expected to be covered comprehensively in the new single Code of Practice from the Regulator, which should be published this summer.

2 Cyber Risk

2.1 Cyber risk can be broadly defined as the risk of loss, disruption or damage to a scheme or its members as a result of the failure of its information technology systems and processes. It includes risks to information as well as assets, and both internal risks (e.g., from staff) and external risks (e.g., hacking, phishing, ransomware.)

2.2 Cyber risk is an evolving area and one that cannot be fully mitigated against. It is therefore important to acknowledge it a threat and have appropriate steps and procedures in place should an event occur.

2.3 There is a multiplicity of cyber threats including ransomware attacks, denial of service, phishing and "zero-day" attacks and they can lead to data loss, financial loss, disruption to service and reputational damage.

2.4 Specific ways the Pension Fund can be targeted include –

- The Fund holds a large amount of detailed personal data that could be exploited either by stealing a member's identity or, due to the quantity of information being held, the data could be accessed with a view to selling it in bulk.

- As the Fund also holds billions of pounds of assets, criminals may try to divert transactions to access these funds. It is also possible that Fund Managers, Pool Operators or other third parties may be targeted due to the large amount of assets that they manage.

- A large amount of member data and financial information is held online which could be targeted to gain access to personal data or bank details.

- The level of cyber security awareness is relatively low amongst scheme members and personal information may be sent in an unsecured email which could be intercepted.

2.5 The consequences of a cyber attack could include disruption to payments, identity theft, reputational damage, loss of members' trust, financial or time loss, fines being imposed by the Regulator.

2.6 The Pensions Regulator is very clear that a fund should not solely rely on the corporate IT team's cyber policies and procedures. Its special guidance expects steps to be taken to build up cyber resilience (i.e. minimising the risk of a cyber

incident occurring and recovering if an incident does occur) through an assessment cycle. Officers have been working with internal teams and third-party providers to understand the management and mitigations in place with regards to cyber risk. This will be put into a Fund specific plan.

3 West Sussex County Council

2.7 The County Council provides the infrastructure which supports financial transactions of the Pension Fund and the network on which files are held.

2.8 The County Council IT Department regularly review, measure and evaluate the corporate and organisational response to current and emerging cyber threats and where applicable take pertinent actions to mitigate any risks identified. The Council has joined South East Group Warning Advice and Reporting Point to assist with ensuring that cyber attacks are identified early, knowledge of current and emerging threats is shared and that reporting and monitoring is effective.

2.9 There are regular communications to all staff regarding cyber threats, particularly phishing scams, and all staff are expected to undertake mandatory annual Information Security and Data Protection training. This is monitored and recorded for Pensions Team members alongside other training undertaken. Pensions Team officers are also required to complete the Pension Regulator Toolkit training which includes a module about pension scams.

2.10 There is a clear and defined testing schedule for the Council including business continuity/disaster recovery, penetration testing and social engineering. The IT Department are also undertaking a training needs assessment to ensure resources are appropriately skilled and corporate practices are aligned to the National Cyber Security Centre guidelines.

4 Hampshire Pension Services

4.1 Hampshire Pension Services (HPS) are the administrators for the West Sussex Pension Fund. They therefore hold a large amount of detailed personal data and generate payments from the Fund's bank account All member pension records and documents are held electronically in UPM, a pension database system provided by Civica.

4.2 The delegation agreement between West Sussex and Hampshire sets out the data protection requirements that Hampshire must adhere to including archiving and backing up data.

4.3 HPS have recently produced a Cyber Security Statement of Compliance which sets out their approach to cyber resilience and which has been shared with officers. It includes how HPS assesses and minimises the risk of a cyber incident occurring but also plans to recover, should an incident take place.

4.4 HPS also have a dedicated webpage informing members about the risks of pension scams and liberation including the warning signs for members to be aware of and the actions that they should take if suspicious. HPS have self-certified to the Pensions Regulator that they follow the principles of the Regulator pledge to combat pension scams.

5 Other Third Parties

5.1 Following the transfer of liquid assets into the ACCESS ACS there is a greater reliance on the systems and processes that Link as the Operator has in place regarding cyber security. There are provisions within the Operator Agreement in place with Link, setting out their responsibilities in this area.

5.2 The ACCESS Support Unit has responsibility for contract management and there is a contract manager in place to ensure that Link comply with the requirements of the Operator Agreement including cyber security and data protection.

6 Training

6.1 The LGPS Online Learning Academy has a section on Introduction to Cyber Risk which sits within Module Six – Current Issues. This provides a brief background to cyber risk and the responsibilities of the Fund.

6.2 The Pension Regulator toolkit consists of seven modules including Managing Risk and Internal Controls and Pension Scams. It is recommended that all Committee members complete the toolkit.

Katharine Eberhart
Director of Finance and Support Services

Contact Officer: Rachel Wood, Pension Fund Strategist, 0330 222 3387, rachel.wood@westsussex.gov.uk

Appendices

None

Background papers

None