LOCAL PENSION BOARD – 24 JANUARY 2020

CYBER SECURITY

Report by the Director of Finance

RECOMMENDATION

1. The Board are RECOMMENDED to note the latest position on cyber security and advise the Pension Fund Committee as appropriate.

Introduction

2. At the last meeting of this Board, it was requested to bring a further report on cyber security to this meeting. This report sets out the risks associated with cyber security both in respect of pensions administration and pension investments and sets out the current approach to the mitigation of these risks.

Cyber Security in Administration

3. Cyber risk can be broadly defined as the risk of loss, disruption or damage to a scheme or its members as a result of failure of its information technology systems and processes. This also includes risks to information (data security); assets; internal risks (staff) and external risks (hacking).

Assessing and Understanding the Risk

4. As a pension administrator, the Fund holds large amounts of personal data for administering and managing the scheme. This data is collected, processed and shared with a large number of individuals and organisations, as detailed on the attached information asset register (see Annex 1).

5. Altair has long been the software used for holding and processing data, but this has changed over time to include:

- Hosting – data is held and processed on Heywood servers which are remote from the Council.
- I-connect is being rolled out to allow scheme employers to upload their data returns directly to Altair
- Member self-service allows scheme members to update certain information directly to Altair and run “what if” calculations on the data we hold.

6. As detailed on the information asset register, the number of organisations with whom information is shared has also increased.

7. The risks to this data can be summarised as:

- Cyber – malware or ransomware

- Loss or misuse of data (GDPR)
- Us! A Government survey found that 50% of information security breaches were caused by inadvertent human error.

Controlling the risks

8. The overall cyber security risks are managed by the OCC IT security protocols as detailed on intranet.

9. For Heywood Altair software, the documentation from Heywood attached as Annex 2 confirms the system accreditation and how the system is monitored and audited. The most recent audit started in November 2019 and will be finalised in February 2020. The most recent available Penetration Test Report is dated February 2019 and is attached to this report as Annex 3.

10. For all other third parties, data is shared either via a secure web portal, or by protected file. In all cases data sharing agreements are signed or included in the contract.

11. All staff are required to sign up to the Acceptable Use of Information Policy and to undertake Data Protection Essentials Training. All team meeting agenda include an item on GDPR. Additionally, a clear desk policy is operated, and all laptops are locked away each evening.

Monitoring and Reporting

12. OCC has a clear system for the reporting and investigating of any data breaches. All team members are aware of these requirements, how they report and record any breaches.

13. In line with data sharing protocols or contractual arrangements suppliers are required to report any breaches and actions taken.

Cyber Security in Investments

14. Cyber security is increasingly recognised as a key and growing issue for companies. The risks in this area are significant and include service interruptions, data access breaches, and data loss which can all have significant financial, operational, and reputational impacts for affected companies. Recent examples are included in Figure 1 below.

15. These risks are only likely to continue as the use of data and online functionality continues to become more embedded in companies' business models across all sectors, and at the same time expectations from regulators, and the fines they can issue, continue to rise.

Figure 1

Example Cyber Security Incidents

In 2018 seven UK banks were subject to a distributed denial-of-service attack that left customers with intermittent access to banking services over a two-day period. As well as the reputational impact direct financial costs were estimated to run into the millions.

In 2019 Facebook were issued with a $5bn fine by the US Federal Trade Commission in relation to the sharing of private user data with Cambridge Analytica. Highlighting the impact for investors, Facebook's market value fell by £119bn (19%) following an announcement of slowing user growth widely attributed to the fallout of the Cambridge Analytica scandal.

16. Recognising the importance of cyber security in investing, Brunel have included it as one of their six priority topics for responsible investment activity. In addition, cyber security is included in one of the 12 key engagement themes for 2019-21 by Hermes EOS, the voting and engagement provider appointed by Brunel. Brunel have also recently contributed to a paper from NEST and RPMI Railpen: *Why UK Pension Funds Should Consider Cyber and Data Security in Their Investment Approach* (https://www.rpmirailpen.co.uk/wp-content/uploads/2018/05/Railpen-Nest-Cyber-Security-Report.pdf)
As well as through engagement Brunel will also be using voting to promote good cyber security governance at companies.

17. Cyber security is increasingly being recognised as a key investment risk by LGPS funds and on behalf of its members the LAPFF undertakes engagements on this topic.

18. As well as the risk to investee companies the Pension Fund also has a strong interest in the cyber security of its fund managers. On an annual basis the Fund receives independently audited internal control reports from its fund managers. These reports include assessments of controls relating to data management, IT systems and infrastructure, and business recovery plans. Brunel are also cognisant of the importance of fund manager cyber security arrangements and so this forms a key part of their due diligence process, including questions on this topic in their tender documents, and their ongoing monitoring of the managers.

Lorna Baxter
Director of Finance

Contact Officers: Sally Fox Tel: 01865 323854
Greg Ley Tel: 07393 001071

January 2020