PENSION FUND COMMITTEE – 10 OCTOBER 2022

CYBER SECURITY

Report by the Director of Finance

RECOMMENDATION

1. **The Committee is RECOMMENDED to comment on the actions proposed in this report and to advise if any other actions should be taken.**

Executive Summary

2. As set out in the most recent edition of the Governance Newsletter, the Pension Regulator has attached a high priority to cyber security. It is their expectation that Committee Members understand cyber risk in the context of their Fund and are happy with the information they are receiving provides them sufficient assurance that these risks are being appropriately mitigated.

3. This Committee previously received an update on the draft documentation, produced by Hymans, setting out the fund's approach to cyber security. An updated version (Annex 1) of that report has been received and reviewed with colleagues in ICT and Information Management. This report sets out where the fund is compliant and what further actions need to be taken.

<u>Policy compliance</u>

4. Paragraph 3 of the attached report refers to the fund's methodology for ensuring compliance as set out in appendix d which has been updated to confirm where responsibilities lie. In practice this has not always been so clearly set out to the team and whilst training and awareness sessions for specific policies / policy changes has been formalised. Action:

- update team of policy champion role.
- Include a standard agenda item at team meeting for policy updates / queries.
- Document specific training sessions

<u>Asset Management</u>

5. The pension services information asset register details the information held within the team and how this is stored and accessed. Colleagues in Information Management Team confirm that these registers do need to be updated. However, no timescales can be given due to staffing levels and proposed structure review. Action:

- Schedule an interim review of the asset register

Configuration Management

6. The process for confirming compliance with policies is one of exception where if ICT identify anomalies or attempts to access system this would be investigated and flagged as appropriate.

Devices

7. ICT confirm that they control access to all devices. In the absence of single sign on there is an internal process to ensure that access to Altair is removed for any leavers from the team. Heywood confirm that the option of single sign on is being considered. Action:

- Continue discussions with Heywood and ICT to move to single sign on.

Malware / Ransomware

8. The current system is that team would be notified if an incident occurred. Action:

- ICT to provide annual report.

ICT enforce the OCC email policy which directs all users to ensure anti-virus system are in operations to prevent virus or malware.

Patching

9. ICT manage this process in background and advise users of any actions they need to take. Given the number of these this is an operational issue, and no reports are provided to senior officers.

Authentication

10. ICT's approach of a single sign on, as referred to in paragraph 6 is not yet available. However, the fund is exploring with Heywood the extension the 2 factor authentication process for when using the public network access. Action:

- To clarify timetable for introduction of 2FA when using public network access.

Access Controls and Passwords

11. In terms of access control managers must complete ICT documents for users to be set up on systems. For Altair managers must write to Systems Manager confirming when new staff are starting and what access they will be given. For staff who are leaving again, managers need to write to Systems Manager.

12. There are policies and procedures available on the intranet for all team members to understand access to OCC when working in different places.

13. The intranet has a lot of information on how to set secure passwords and how to keep passwords safe. The biggest challenge is in ensuring that these are followed by all team members. Action:

- To review records held by System Manager
- Use team meetings to keep all team members trained and up to date with policies.

Bulk data / Personal data

14. ICT has reviewed the fifteen measures of good practice outlined on the National Cyber Security Centre and has commented that items 11 (alert to atypical access attempt) and 14 (no possibility of administrative access through spear-phishing) are weaknesses in the absence of a single sign on as mentioned in paragraphs 6 and 9.

15. The data sharing policy is written and maintained by Information Management Team who have confirmed that this is to be reviewed shortly. However, no timescales can be given due to staffing levels and proposed structure review.

Security Monitoring and Testing

16. Penetration testing is carried out annually with the next review due in January 2023. Action:

    1. ICT will provide fund with a copy of the penetration test report.

People Centred Security and Phishing

17. ICT software stops side-lines suspect emails so that users can review these to decide whether the email is genuine and can be forwarded to the inbox or whether this should be deleted. There is an established procedure for any suspect emails to be reported. To strengthen these controls from October 2022 ICT are introducing test phishing emails across OCC.

Remote Working

18. A remote working policy was issued in May 2021.

Social Media

19. The social media policy was last updated in June 2022

Certification

20. Report has been updated.

Third Party Suppliers

21. The policies, procedures and actions above largely focus on the cyber risks within our own ICT environment. However, we are heavily reliant on third party suppliers, which the majority of pension benefit and investment data held on third party's systems. Our approach in this area is to ensure that our third party contracts contain standard cyber clauses to protect the Fund in the same way our policies and procedures aim to protect the Fund where the data and systems are managed in-house. Not all our older contracts include these standard clauses. Action

- Review all third-party contracts to ensure standard clauses are included
- Where standard clauses not present, ensure the supplier has their own robust arrangements to mitigate against cyber risk and protect the Fund's data and our access to the core systems to fulfil the Fund's statutory duties
- Ensure all suppliers provide an annual report on compliance with cyber policies and procedures and the results of all security checks

Conclusion

22. Overall, the policies and processes for managing cyber security are in place. However, this report has highlighted the need to clearly understand and document where the various responsibilities lie and the need for better communication between all parties to ensure that systems are compliant and protected.

23. Within the team communications and training need to be scheduled more regularly so that understanding and actions are better understood, and any risks are mitigated.

24. Further actions needed are to review the business continuity plan and review risk register entries, in line with the above.

Annex:	Hymans draft report on Cyber Security
Contact Officer:	Sally Fox Pension Services Manager Tel: 01865 323854

August 2022