PENSION FUND COMMITTEE – 03 MARCH 2023

CYBER SECURITY REPORT

Report by the Director of Finance

RECOMMENDATION

The Committee is RECOMMENDED to

a) To review this report and determine any further actions to be taken
b) To confirm that this report is to be produced on an annual basis
c) To decide if pension specific fund penetration testing should be carried out

Introduction

1. This report reviews the actions taken to date and sets out future plans to review and update the fund's cyber security.

Initial Review

2. In May 2022 the fund's actuaries Hyman Robertson carried out a review of the fund's cyber risk prevention and response approach. Following a review of the documents provided a workshop was held to:

- Explore participants' current understanding of the fund's business continuity plan in the event of a cyber incident, and
- Explore the policies and procedure in place which are designed to reduce the likelihood or impact of a cyber event occurring.

3. The findings and actions from this meeting were:

- To consider updating the business continuity plan to provide more explicitly for cyber-attack.
- Council policies contained many basic cyber controls, but these were not always acknowledged as part of the fund's cyber response.
- Protections provided by the Council's Information and Technology Management were not always clearly documented or acknowledged as part of the fund's cyber response.
- Determine what additional reporting, or assurance is available from the Council's Information and Technology Management relating to their actions to safeguard systems and monitor suppliers.
- The fund should consider improving restricted access to information and reduce key man risk in relation to systems knowledge.

- Regular meetings to be arranged with the Council's Information and Technology Management team.
- The fund to review its compliance with relevant policies and take steps in relation to information access management and systems training.
- Regular review of the fund's risk register should include consideration of the impact of the completion of these actions.

4. Hymans Robertson produced a further, more detailed report, in July 2022. A report and this document from Hymans Robertson were included on the agenda in September 2022, which set out the following actions to be taken:

- Update team of policy champion role.
- Include a standard agenda item at team meeting for policy updates / queries.
- Document specific training sessions
- Schedule an interim review of the asset register
- Continue discussions with Heywood and ICT to move to single sign on.
- ICT to provide annual report re ransomware / malware
- To clarify timetable for introduction of 2FA when using public network access.
- To review records held by System Manager
- Use team meetings to keep all team members trained and up to date with policies.
- ICT will provide fund with a copy of the penetration test report.

Progress to Date

5. One of the key actions since September has been the review of the fund's supplier cyber security arrangements. Information from the suppliers, which was reviewed by the Council's Information and Technology, was reported to the Committee in December 2022. At the time of writing that report there was one supplier's information outstanding. This has now been received and is with Council's information and Technology for review.

6. Team training has been undertaken and cyber security is now a standard agenda item at team meetings. The intention here is to include an annual training session for all team members.

7. Quarterly meetings have been set up with the Council's Information and Technology to ensure that the fund's processes are kept under review. Colleagues in the Council's Information and Technology have confirmed:

- That penetration testing has been undertaken with nothing to report.
- That producing a list of patches / security updates is not feasible given that there have been over 70 patches for Microsoft Edge alone in the last year.

8. Pension specific penetration testing could be carried out, but this would be at cost to the fund.

9. The main outstanding action is that of finalising the documentation so that all relevant information is in one place.

Threats and Breaches

10. No targeted or successful attacks were encountered during the period. This information will be reported annually except for any incidents which occur during the year.

Risks

11. Discussions are continuing with the fund's software supplier Aquila Heywood regarding single sign on, which is due to be implemented during 2023.

12. The last fund technology audit was carried out in 2016. Audit has contacted officers and the fund is now included in the audit plan proposal for 2023. Confirmation of if the fund is included will be confirmed in April.

Conclusion

13. The key systems and controls are in place with a mechanism to review this information on a quarterly basis.

Contact Officer: Sally Fox - Pension Services Manager - Tel: 01865 323854
Email: sally.fox@oxfordshire.gov.uk February 2023