Oxfordshire Pension Fund

DRAFT - Approach to cyber risk

July 2022

Susan Black and Claire McDines

For and on behalf of Hymans Robertson LLP

Contents

1 Introduction

This document summarises the approach of Oxfordshire Pension Fund ("the Fund") to dealing with cyber risk. This document will be reviewed annually to ensure that it meets the Fund's needs.

Having an approach document:

- Ensures visibility of key systems and processes at risk.
- Signposts available tools and documents to manage this risk.
- Records key roles and responsibilities in the instance of a cyber risk event occurring.
- Details training available to officers and other stakeholders.
- Records the monitoring and reporting requirements.

This document also provides context in relation to cyber risk.

2 Context to cyber risk

Cyber risk can be defined as:

> *"any risk of financial loss, disruption, or damage to the reputation of the Fund or its members resulting from the failure of its IT systems and processes. "*

Breaches in cyber security may occur as a result of:

- deliberate and unauthorised action by someone making a concerted effort to infiltrate systems and access data,
- unintentionally through carelessness, for example sending data that's not encrypted or leaving passwords expose; or
- operational risks due to poor system integrity and lack of prevention software and procedures.

Cyber risk is on the Fund risk register in recognition of the high value of assets, high value transactions, and the scale of personal data held.

3 Prevention

There is a suite of policies and procedures in place to mitigate cyber risk. A full list of the Fund's policies relating to cyber and data controls can be found in Appendix D. The Fund's methodology for ensuring policy compliance is also set out in Appendix D.

Ownership and day to day management of the Fund's cyber approach is carried out by the Pension Services Manager in collaboration with Oxfordshire County Council's (OCC) ICT and Information Management Teams. ICT and Information Management Teams ensures that all policies are up to date and the controls within these policies are adhered to. Full key contact details are at Appendix A.

Key areas in the Fund's cyber approach are summarised by the sections below, with reference to the existing OCC policies and procedure adopted by the Fund. Nothing in this document replaces or supersedes the OCC polices in place.

Asset management

This is the process of identifying the assets that present a security risk. Assets include any data that needs to be configured or managed, such as personal member data, payroll data and financial capital. It also includes technology, both hardware and software, and physical locations. To be effective, the asset management process needs to be carried out in a reliable and timely manner.

In accordance with the OCC Information Access and Protect Policy the Fund maintains inventories of information assets and has identified that key assets include:

- [member personal data]
- [insert additional]

Configuration management

This is the process of maintaining the details of the Funds' computer systems and other assets. The Fund has a dependency on the OCC ICT Team who control the hardware and computer systems used by the Fund and provide security configuration and firewalls etc. The Fund has adopted and adheres to the OCC Information Access and Protection Policy and the OCC ICT Access Policy which contain controls in relation to who at the Fund can access systems, applications and equipment.

Devices

All devices used by the Fund are supplied and controlled by the OCC ICT Team. In addition to the control of user access to devices there are also regulations around acceptable use withing the ICC Acceptable Use Policy. For example, all data stored on removable media devices must be encrypted to a level approved by ICT Services. Any images taken on council mobile phones must be transferred to the council's network and deleted from the mobile phone as soon as possible.

Cloud

Cloud computing is the delivery of hosted services over the internet, where shared computing and storage resources are accessed as an online service. The Funds' Altair Pensions systems are hosted by means of the Cloud.

The OCC Information Access and Protection Policy and the OCC ICT Access Policy are in place at the Fund and contain controls in relation to the use of Software applications (including Cloud based applications and websites), for example downloads and uploads should only be loaded onto a Council machine by staff from Digital and ICT Services.

Malware/Ransomware

Malware (short for "malicious software") is an umbrella term that describes any malicious program or code that is harmful to systems. It is typically delivered over a network, that infects, explores, steals or conducts virtually any behaviour an attacker wants. There are numerous methods to infect computer systems because malware comes in so many variants. Ransomware is a type of malware designed to deny a user or organization access to files on their computer. By encrypting these files, threatening to publish the victim's personal data or perpetually block access unless a ransom is paid for the decryption key.

The OCC ICT have software in place to lessen the chance of malware and ransomware attacks, and information on the efficacy of this software will be provided to the Fund on an annual basis.

There are also controls in place around the use of ICT equipment and software to further reduce risk. For example, as referenced above software applications (including Cloud based applications and websites) and downloads and uploads should only be loaded onto a Council machine by staff from Digital and ICT Services.

The Fund complies with the OCC Email Policy which directs that to assist in prevention of viruses or malware, all users must ensure an anti-virus system is in operation.

Patching

Patching is carried out to apply updates to Fund devices and software in order to improve security and/or enhance functionality. When patches are carried out by the Council ICT staff, there is no reporting to officers of the fund.

Authentication

The process of authentication provides assurance and confirmation of a user's identity. Authentication has further expanded in recent years to require more information of the user, before a user attempts to access information stored on a network, he or she must prove their identity and permission to access the data.

The Fund is currently in the process of arranging 2 factor authentication for public network access. This timetable is to be finalised.

Access control and passwords

There is a system for controlling who can access data and systems. OCC ICT staff operate the technical controls over systems access however the senior officers and team leaders at the Fund determine who access should be permitted to. All system users have a responsibility to protect their access details and only use systems as permitted. Full details can be found in the ICT Access Policy. For example, passwords provide the first line of defence against any unauthorized access to the Funds data. In addition to the technical controls around password creation as detailed in the ICT Access Policy, users are also instructed to follow password guidelines, for example '*never reveal passwords to anyone'*, '*never write passwords down'* and 'do not use the same password to access different County Council systems'.

Bulk data/Personal data

Personal data is defined as '*Information that relates to an identified or identifiable individual, such as a name or number, or information such as an IP address*.'

The Fund holds and processes bulk member data, and other personal member data, on a regular basis. This data is of a sensitive nature and therefore must be kept safe. The OCC Data Sharing Policy details how data should be handled and is followed by the Fund.

The fifteen good practice measures listed below have been considered as part of the Funds approach to bulk data. Full detail of these measures is outlined on the National Cyber Security Centre.

1 Know your data

2 Keep only essential data

3 Unmitigated vulnerabilities

4 User access and privilege

5 Administrator access

6 Know your external dependencies

7 Audit data access

8 Prompt mitigation

9 No unsupported software

10 Detecting compromise components

11 Automatic alert to atypical access attempt

12 Well defined interfaces

13 Rate-limited user access

14 No possibility of administrative access through spear-phishing

15 All backups held securely

Security monitoring and testing

Detecting (and responding to) activities that could represent a security incident. Also known as protective monitoring is carried out regularly by ICT staff further details can be found in **section 9** of this report.

As a means of testing the Funds computer network/system for security weaknesses so that they can be fixed, regular authorised tests are carried out. Penetration tests are carried out every year, results are collated and presented to the fund by ICT.

People centred security and phishing

Cyber criminals frequently employ human psychology in their attack strategies, it is for this reason the Fund treats cyber awareness as an upmost priority within their policies and training plans. Details of the training provided to officers and all stakeholders can be found in **section 8** below.

Phishing are a type of attack were untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website. The OCC ICT have software in place to catch such emails however this type of software isn't 100% effective therefore non-technical controls are also in place to further mitigate the risk. For example, the Email policy states that users must report any suspect emails or attachments to the ICT Service Desk.

Remote working

Policy issued in May 2021

Social media

Policy updated in June 2022

Certification

PSN Certification for OCC

NHS Data Security and Protection Toolkit are used as very comprehensive.

4 Response

In the event of a cyber security incident the Fund would collaborate with OCC who would lead the Incident Response.

The Fund's Business Continuity Plan would be used to ascertain key information and drive decision-making.

As set out in the Fund's Business Continuity Plan:

- The key Fund contacts involved in a cyber security incident are set out in section A].
- The key Fund systems and suppliers are set out in sections B.

The key phases and steps of an incident response are summarised below and will be used by the Fund to ensure the Business Continuity Plan (BCP) is a robust source of information.

Preparation

Triage – The initial stage is to assign a Lead Officer to work with the OCC Incident Manager to ascertain if the event warrants being treated as a security incident. As part of triage, the Lead Officer should gather pertinent information, assess severity, and categorise risk.

Escalate – Depending on the above assessment an escalation may be required in line with the OCC incident response process. The key contacts set out in the BCP should be leveraged. This should also be monitored in case further escalation is required further down the line.

Kick off response – At this stage the Incident Response team may need contact internal or external parties who need to be involved and cascade details of required action. Contact details are contained within the Fund BCP.

Reporting –Where a data breach may have happened the Data Protection Officer should be informed in line with the OCC Data Protection Policy. The decision will need to be made as to whether any GDPR breach has occurred and if so whether a report needs to be made to the ICO. Other parties who may need to be informed are S151 officer, Chief executive, OCC Media Team, Pensions Committee and Board and TPR.

Core response

The Lead Officer will be crucial in the following steps:

Analyse – This should involve technical analysis but also impact analysis and reputational risk management. Initial priority is to understand enough to take containment/mitigation actions and remediate the attack. Prioritisation of tasks is crucial, as is assigning ownership of these tasks. These priorities should also be constantly reviewed and modified as required.

Contain/Mitigate – Steps should be taken to reduce or limit the impact of the incident and prevent further risk or spread. This can involve both technical and non-technical actions for example isolating systems, blocking network activity, media handling and updates to public websites. It is important to consider the impact of any decisions made both good and bad.

Remediate/Eradicate – This stage is similar in actions to the containment stage but with the aim to fully remove the threat. It is important to confirm that remediation has been successful before moving to the recover stage - this may involve monitoring for a period. Some analysis may continue in this stage too.

Recover – When the incident response team confirm that business environment has returned to a risk-free state, they will recommend a return to 'business as usual'. This should only proceed when the incident is believed to have been contained and consequences understood. This may include final actions taken to handle regulatory, legal, or PR issues.

Review and close down

Following the successful recovery from an incident, the OCC Incident Response Manager may arrange a post incident review, attended by members of the incident response team including the Lead Officer.

The post-incident review may consider:

- Pre-event - circumstances that led to the event
- Post event - response activities

Pre-event review considerations

- What would have prevented the incident from occurring?
- How could we have detected the events sooner?
- Is this something considered by our cyber risk assessment?

Post-event review considerations

- What would have made our response more effective/efficient?
- What was the key thing that led to us understanding the incident?
- How long did it take to detect the incident?
- What systems were impacted?
- Was any information difficult to obtain?
- Were the right people and tools available?
- Did we have any communication issues?
- Were there any weaknesses in the response which need addressed?

5 Appendices

Appendix A - Key Contacts

Roles and responsibilities

The core incident response team should include a member of ICT and Senior officer in the first instance. Depending on the type and scale of the event deputies may substitute.

In the event of a cyber incident the key required contacts are listed below [full details required from officers]

Department	Contact name	Contact number	Contact Email
Senior Fund Officer	Sean Collins	07554103465	Sean.Collins@Oxfordshire.gov.uk
Pension Services Manager	Sally Fox	07776997052	Sally.Fox@Oxfordshire.gov.uk
Systems Manager	Rachael Salsbury	07825314783	Rachael.Salsbury@oxfordshire.gov.uk
ICT	Asher Sims	07500977798	Asher. Sims @oxfordshire.gov.uk
Legal	Anita Bradley		Anita.Bradley@oxfordshire.gov.uk
DPO	Simon Harper	07873700331	Simon.Harper@oxfordshire.gov.uk
Information management	Simon Harper	07873700331	Simon.Harper@oxfordshire.gov.uk
S151 officer	Lorna Baxter	07393001218	Lorna.Baxter@oxfordshire.gov.uk

Appendix B – Key Systems

System	Purpose	Controller/Supplier	Contact
Network access	**to enable access to all systems**	OCC	Asher Sims / ICT helpdesk
Altair	**For pension payroll; calculation and payment of all benefits**	Heywood	TBC
MSS	**For members to access documents uploaded by team and to view information about their pension**	Heywood	TBC
I-Connect	**To enable scheme employers to upload monthly payroll information to Altair**	Heywood	TBC
PT-X	**To make BACS payments**	Bottomline	TBC
Gemalto	**To make BACS payments**	OCC	Asher Sims / ICT helpdesk
SAP	**To upload and access accounting information**	OCC	Asher Sims / ICT helpdesk
Microsoft office	**To produce documents from Altair**	OCC	Asher Sims / ICT helpdesk

Appendix C - Key Suppliers

List suppliers and speak to info management about what assurance they have.

Heywood

Bottomline

Appendix D – Policies and Procedures

The following table details all relevant policies currently in place to protect the fund from cyber risk.

Policy	Policy Owner	Fund Policy Champion	Policy Compliance Check Due Date
Acceptable use policy Access to (oxfordshire.gov.uk)	Simon Harper	Sally Fox	TBC
Access information security vetting policy Access to (oxfordshire.gov.uk)	Simon Harper	Sally Fox	TBC
Data protection policy Access to (oxfordshire.gov.uk)	Simon Harper	Sally Fox	TBC
Data sharing policy Access to (oxfordshire.gov.uk)	Simon Harper	Sally Fox	TBC
Email policy Access to (oxfordshire.gov.uk)	Simon Harper	Sally Fox	TBC
ICT access policy Access to (oxfordshire.gov.uk)	Simon Harper	Sally Fox	TBC
Information access and protection policy Access to (oxfordshire.gov.uk)	Simon Harper	Sally Fox	TBC
Information security incident policy Access to (oxfordshire.gov.uk)	Simon Harper	Sally Fox	TBC
Security classifications policy Access to (oxfordshire.gov.uk)	Simon Harper	Sally Fox	TBC
Data retention policy	Sally Fox	Sally Fox	TBC

Fund Policy Champion Role

The Policy Champion is responsible for:

- Dealing with policy queries from the rest of the team
- Ensuring any changes to policy are noted and communicated and any process changes implemented
- Providing feedback to the Policy Owner to drive changes or exceptions to policy which are needed by the Fund
- Undertaking proportionate activity to ensure that the policy is understood and followed by the team. This could include, but is not limited to:
    - Carrying out training and awareness sessions with the team
    - Carrying out checks and documenting the results to ensure that policy compliance can be reported, and actions identified and take to improve results where necessary.

Appendix E - Training

All officers of the Fund receive training as below…

Mandatory training (officers)

Acceptable use of equipment and information

Business continuity

Confidentiality

Corporate governance

Data protection

Freedom of information

Guidance on secure working practices

Social media

Additional training based on role

Cyber security

TPR website

Training for other stakeholders

Members, employers, Committee and Board members

Monthly newsletter

Training sessions ahead of quarterly meetings

Hymans online learning academy

TPR website

Annual knowledge assessment

Appendix F - Monitoring and Reporting

The risk to the Fund is an evolving threat which needs to be monitored. As such it has been decided that a full report on cyber monitoring should be provided to the Pension Committee and Pension Board on a annual basis. This report should contain details of:

- key digital assets,
- any cyber threats or data breaches over the period,
- a list of patches or other security updates applied by OCT,
- log of penetration testing carried out and results,
- any perceived risks or gaps in controls and how these are being mitigated.

Prepared by:-

Susan Black and Claire McDines

21 July 2022

For and on behalf of Hymans Robertson LLP