Cyber security

Considerations for pension schemes

Cyber security is crucial for pension schemes, given the nature of the data and information held and the evolving risks of a cyber incident. In the following pages, we have included some helpful questions for you to consider.

Pension scheme trustees may wish to prioritise the following critical questions before exploring the more detailed checklist overleaf. By focusing on these key aspects initially, trustees can address the fundamental areas and lay the groundwork for a more comprehensive approach to cyber security.

- Do you **understand** your cyber risk?
- What **controls** do you have in place?
- Have you **assessed** your cyber footprint?
- If presented with an incident right now, **what would you do?**

LCP can help you prepare for, reduce, and react to the cyber risks threatening your scheme

- The **checklist overleaf** enables you to assess how prepared your scheme is, compared with the Pensions Regulator's guidance on cyber security.
- We offer **tailored scenario planning** training to help you prepare and practice your incident response. We also provide **introductory training**, brought to life with case studies and recent examples.
- We can assist you with **assessing** and **understanding** your scheme's **cyber risk**, such as assessing your cyber footprint, **ensuring** controls are in place, review of risk management activities and the preparation of a cyber security policy,
- Cyber controls should be considered in the context the wider **General Code of Practice**. Speak to us about gap analysis, training and preparing for your ORA.

Useful resources:

Cyber risk

The Pension Regulator's cyber security principles
ICO guidance on data security
The National cyber security centre
NCSC 10 steps to cyber security
PLSA cyber risk made simple guide

*Have a mindset of "**when**" rather than "**if**"*

General Code

Understanding the General Code of Practice: LCP's guide to the ESOG
Own Risk Assessments: LCP and PLSA's made simple guide

Cyber security checklist

Checklist for pension scheme trustees

This generic checklist is a reference for pension scheme trustees. It is intended to assist you with identifying actions you should consider in respect of cyber security.

	Yes / no	Notes or actions required
Assess and understand the risk		
1. Do the trustees have appropriate knowledge and understanding of the cyber risks facing the pension scheme? For example: a. Are the potential operational, reputational, financial impacts of a cyber incident on your scheme and sponsor understood? b. Is the likelihood of different types of breaches understood (e.g. accidental / human error, ransomware, phishing)? Do the trustees receive cyber security training at an appropriate level and frequency?		
2. Do the trustees understand the need for confidentiality, integrity and availability of the systems and services for processing personal data, and the value of the personal data processed within them?		
3. Has data mapping been completed and are the trustees aware of the scheme's cyber footprint both in terms of *data* (i.e. what information is held, where is it stored, how is it accessed and which information is shared with whom) and *assets* (i.e. where assets are held and how investment instructions are issued and verified)?		
4. Is cyber risk on the risk register? Are roles and responsibilities in relation to cyber risk clearly defined?		
Ensure controls are in place		
5. Do the trustees have a cyber security policy?		
6. Does the sponsor have a cyber security policy? Does the sponsor have any internal requirements for the trustees/pension scheme that need to be considered, communicated and assessed?		
7. Do the trustees have a response plan in place to deal with any cyber incidents? a. Are responsibilities for dealing with a cyber incident clearly articulated and assigned within the scheme? b. Do the trustees have policies to assess whether data breaches (which may arise from a cyber incident) need to be reported to the Information Commissioner (www.ico.org.uk)? Are these coordinated with the trustees' data protection policy and data breach response plan? c. Does this include consideration of crisis communications to members and use of legal privilege? d. Is a log kept of data breaches and cyber incidents and is there a process for post-incident review?		

	Yes / no	Notes or actions required
8. Do all key parties (trustee board, key advisers, sponsor) involved in the pension scheme have appropriate business continuity plans which include detection and reaction to cyber incidents?		
9. Have the trustees satisfied themselves with their third-party providers' controls and accreditation? Are the trustees aware of the relevant certification advisers would typically hold (e.g. Cyber Essentials or ISO 27001 certification)?		
10. Do the trustees have access to a specialist they can turn to if required, either via the sponsor, insurance or a third party?		
11. Is cyber security an active consideration in the selection of advisers / providers?		
12. Are critical systems and data regularly backed up? Is the integrity of backups tested?		
13. Is the pension scheme compliant with data protection legislation?		
Monitor and report		
14. Are cyber risks regularly reviewed (i.e. at least annually or more frequently if there are significant developments)?		
15. Do the trustees assess at appropriate intervals, the vulnerability to a cyber incident of the scheme's key functions, systems and assets (including data assets) and the vulnerability of service providers involved in the running of the scheme?		
16. Do the trustees take action to ensure that policies and controls remain effective and update themselves on cyber security trends and best practices?		
17. Are the trustees clear on how and when incidents would be reported to them and others including regulators?		
18. Do the trustees receive regular reports from service providers on cyber risks and incidents?		
19. Do the trustees understand what, if anything, their internal or external auditors are looking at in relation to controls around the scheme's cyber risks?		
20. Do the trustees regularly review business continuity plans and monitor ongoing compliance and developments in this space?		
21. Have the trustees considered sharing insights and experiences with trusted stakeholders and peers?		
Reducing the financial impact		
22. Does the trustees' liability insurance cover claims relating to cyber incidents? Has the policy been reviewed for any specific exclusions? Is the pension scheme included on the sponsor's D&O (Directors' and Officers') insurance, and if so, can the trustees claim against the D&O insurance in respect of a cyber incident?		
23. Do supplier contracts have adequate provisions regarding GDPR and / or cyber security?		

	Yes / no	Notes or actions required
Trustee cyber hygiene		
24. Do the trustees have policies for the use of devices, and for home and mobile working? Including: a. use of multi-factor authentication b. use of web-based email accounts c. sharing of personal information, meeting papers, use of signatures etc		
25. If e-signatures are used for investment and other instructions, have the trustees considered how easy it would be for a cyber-criminal to obtain and use these to commit fraud?		
26. Have the trustees considered how they would manage their incident response if they could not access email or electronic board papers?		
Member considerations		
27. Have the trustees considered how they might update members if a cyber incident were to occur and could not be resolved immediately?		
28. Have the trustees considered including further warnings on phishing and other cyber risks to member communications in addition to any warnings relating to pension scams? For example, information on the scheme's agreed method of communication with members (e.g. not by text or cold calling) and what data would/would not be requested by the scheme?		

Contact us

To find out more contact any of the below or your usual LCP contacts

Peter Shaw
Principal
+44 (0)207432 7781
peter.shaw@lcp.com

Chris Holly
Partner
+44 (0)207432 6761
chris.holly@lcp.com

This generic checklist has been prepared free of charge as a reference for trustees. It is based on the Pensions Regulator's cyber security principles for pension schemes (link above) and should be read in conjunction with these. It has not been prepared by cybersecurity experts, does not constitute advice, and should not be relied upon for any purpose by any party. This checklist is shared on a confidential basis unless we agree otherwise in writing.