Sackers

Hot topic

February 2024

Cyber security – is your scheme prepared?

TPR's new general code of practice is expected to come into force in late March 2024 and contains a new module on cyber controls. With some recent high profile cyber-attacks in the pensions industry, this is a good opportunity for trustees to take stock of all things cyber.

Trustees must (subject to limited exceptions) establish and operate an effective system of governance including internal controls. These controls need to include measures to manage cyber risk. The new general code sets out TPR's expectations for trustees in respect of cyber risk.

TPR published updated cyber security guidance at the end of 2023, setting out some more practical steps that trustees can take.

What is cyber risk? ?

Cyber risk can be broadly defined as the risk of loss, disruption, or damage to a scheme, or its members associated with using information technology. Risks can arise not only from the technology itself but also from the people using it and the processes supporting it. It includes risks to information (data security) as well as assets, and both internal risks (for example, from staff) and external risks (such as hacking).

What do trustees need to do?

TPR's guidance expects trustees to:

- ✓ Understand the scheme's cyber risk
- ✓ Ensure that the scheme administrator (and others handling scheme data) have appropriate controls in place
- ✓ Manage incidents that arise

Cyber security – is your scheme prepared? cont.

Your path to cyber resilience

Cyber controls should cover people, processes and technology and be proportionate to your cyber risk. Larger schemes, and those more exposed to cyber risk, will need more robust controls. However, the steps below give a good starting point for all schemes on their path to cyber resilience.

Take specialist advice!

You should make sure you have access to the required skills and expertise to assess and manage your scheme's cyber risk. Some schemes may be able to call on such expertise from their employer, while others may need to seek specialist advice.

1 Understanding your scheme's cyber risk

- Organise a cyber security training session for the trustees
- Know your scheme's "cyber footprint". This is the digital presence of all parties involved in your scheme – so the trustees and scheme administrators and, potentially, employers and / or other service providers (eg actuaries, investment consultants, lawyers) or members (eg if you have a scheme website)
- Check your data map – which service providers hold what scheme data and understand the data flows between parties
- Understand what is covered by any insurance your scheme has in place

2 Ensuring controls are in place – working with others

- Seek assurance and / or evidence that providers have the right controls in place. These should cover staff training, data security, technical controls, detecting incidents and response planning
- Check what is (and isn't) covered by any audits, tests or accreditations in place
- Agree (and receive) regular reports in plain English from relevant parties on cyber threats and how emerging cyber risks are being controlled

3 Ensuring controls are in place – trustee processes

- Ensure cyber risk is on your risk register and is reviewed regularly – at least annually and when there are substantial changes to the scheme's operations (eg a new IT system)
- Keep records on how you have assessed cyber risks and the steps taken to ensure the right controls are in place
- Test your incident response plan with a range of scenarios

4 Managing incidents that arise

- Have your own incident response plan in place (stand alone or part of business continuity plan)
- Check that others' response plans (eg employer and administrator) appropriately cover the scheme
- Understand how the scheme's core services (eg pensioner payments) are covered and how / when they will be back online following a cyber incident

Sacker & Partners LLP
20 Gresham Street
London EC2V 7JE
T +44 20 7329 6699
E enquiries@sackers.com
www.sackers.com

For further information, please speak to your usual Sackers contact.
You can also visit www.sackers.com