CONDUENT

FYI® Alert
For Your Information®

UK

Volume 2018 | Issue 22 | 18 April 2018

Cyber Security Principles for Pension Schemes

With the impending introduction of the General Data Protection Regulation (GDPR), the issue of data security has never been a higher priority for trustees of pension schemes and other data controllers and processors.

The Pensions Regulator has now published guidance on cyber security issues that sets out good practice for pension schemes, which trustees can adopt proportionately to the profile of their scheme.

Background

The attraction of pension schemes to fraudsters and other criminals is clear. Pension schemes hold huge amounts of personal data and assets – some £3.3 trillion worth of assets. Add to this the frequency by which data and assets are transferred between parties involved in the running of pension schemes, and the result is that trustees of all schemes must ensure that appropriate steps are taken to ensure that all scheme property is secure, and this includes protection against cyber security risks.

Cyber risks can be broadly defined as the risk of loss, disruption or damage to a scheme, or its members, as a result of the failure of its information technology systems and processes. It can include risks that are accidental, or staff-related, as well as hacking, malware, ransomware, phishing attempts, and co-ordinated DDOS (distributed denial of service) attacks.

Trustees are required to establish appropriate internal controls to ensure that a scheme is run in accordance with both the scheme rules and legislation. A key part of internal controls is ensuring processes exist to identify, evaluate and manage risks. The Regulator quite rightly sees increasing cyber resilience as an example of adequate internal controls.

What does the Regulator expect of trustees?

Trustees must take steps to build their “cyber resilience”. This is the ability to assess and minimise the risk of a cyber incident occurring, but also to recover when an incident takes place. Trustees should work with all relevant parties (such as third party service providers and sponsors) to define an approach to managing this risk.

The Regulator's good practice guidance suggests a three-stage approach (which it calls a cyber risk assessment cycle):

- assessment and understanding of cyber risks;
- putting controls into place; and
- ongoing monitoring and reporting.

Trustees are expected to ensure that all roles and responsibilities are clearly defined, assigned and understood.

Stage of the cycle	Issues for trustees	Particular trustee considerations
Assessing and understanding risks	Are the cyber risks affecting the scheme understood?	• Key functions, systems and assets (including data assets). • Potential operational / reputational / financial impact of a cyber incident on the scheme (and the sponsor, where appropriate). • The likelihood of different cyber breaches occurring. • The scheme's 'cyber footprint' (the scheme's digital presence and the risk posed by all parties, including the trustees, sponsoring employers, advisers, and members).
	Is cyber risk included on the scheme's risk register and is it reviewed at least annually (or sooner following any major changes to scheme operations)?	Changes could include a new IT system or a change in administrator.
	Is there access to the right skills and expertise to understand and manage the risk?	Regular training can be arranged.
Putting controls in place	Are sufficient controls in place to minimise the risk of a cyber incident occurring?	• IT security controls. • Processes. • People involved with the scheme.
	Have the scheme's 3rd party providers and advisers' controls been checked?	Consider cyber security when selecting new advisers and service providers and check contracts.
	Does the scheme have any standards or accreditations available to help demonstrate cyber readiness and has the scheme's cyber risk management been independently assessed?	Trustees also need to check whether the scheme's 3rd party providers and advisers rely on any standards / accreditations.
	Is a response plan in place to deal with any incidents that may occur to enable the swift and safe resumption of operations (see below)?	Trustees also need to check whether the scheme's 3rd party providers and advisers have a response plan.
	Is the scheme compliant with existing data protection legislation (and prepared for the General Data Protection Regulation (GDPR))?	Trustees should ensure there are clear policies on what potentially sensitive scheme information can and can't be sent to their personal email addresses etc.

Stage of the cycle	Issues for trustees	Particular trustee considerations
Ongoing monitoring and reporting	Are the controls, processes and response plans regularly reviewed and tested?	Trustees should establish an incident response plan.
	Is it clear when and how incidents would be reported to the trustees and other parties, such as regulators?	
	Are regular updates provided on cyber risks, incidents and controls?	The National Cyber Security Centre and the Information Commissioner's Office provide guidance.
	Is there a regular source of up to date information and guidance on cyber threats?	Trustees can share information and experiences with trusted stakeholders and peers.

Due to the evolving nature of cyber risk, each of these three stages should be regularly reviewed to ensure the scheme's internal controls remain relevant and up to date.

Incident response plans

In addition to ensuring that systems and processes are in place to ensure the safe and swift resumption of operations, trustees should ensure that an incident response plan is in place, setting out:

1. The roles and responsibilities of the incident response team (to ensure that the scheme has access to sufficient capability to investigate a cyber incident).
2. Critical functions (e.g. payments of benefits) and processes, and what assurances need to be in place before these come on board.
3. In-crisis communications including how and when reporting will be made to trustees.
4. The process, thresholds and time limits for notifying other parties including the Information Commissioner's Office, the Pensions Regulator, or the Financial Conduct Authority as appropriate, law enforcement (in cases of fraud), third parties, and if necessary, scheme members.

The plan should cover a range of scenarios, based on the scheme's assessment of key functions and assets, and the likelihood of different types of incident.

Trustees should ensure that they understand their advisers and 3rd party providers' incident processes, including how and when they would be informed of a cyber incident occurring. Incidents should be documented and major incidents should be followed by a post-incident review, with plans updated in light of experience.

In Closing

While data security should be a high priority for trustees as part of the preparations for GDPR, there is a danger of pension schemes not fully recognising cyber risks (in whatever form). Some trustee boards will have already considered cyber security as part of this work, but many may not have as yet.

Just because a pension scheme is unaware of a cyber-attack, does not necessarily mean that something hasn't happened, especially where trustees have not taken steps to prepare, assess, and monitor cyber risks. The sheer amount of data and funds held means that sooner or later, pension schemes will become a target. This is perhaps unlikely to involve the high profile DDOS attacks faced by some high profile corporate entities in recent years, but lower level risks, such as hacking, phishing, and staff-related attacks cannot be discounted.

As with all risk management, preparation and ongoing monitoring is key.

Authors
John Dunkley, Senior Technical Consultant
Nikki Williams, Senior Technical Consultant

Produced by the Knowledge Resource Centre
The Knowledge Resource Centre is responsible for national multi-practice compliance consulting, analysis and publications, government relations, research, surveys, training, and knowledge management. For more information, please contact your consultant or call us on 0800 066 5433.

CONDUENT