THE
NATIONAL LAW REVIEW

Pensions Administration Standards Association Publishes Guidance on Cybersecurity

Article By
Garon Anthony
Squire Patton Boggs (US) LLP
Compensation and Benefits: Global Insights

- Global
- Financial Institutions & Banking
- Communications, Media & Internet

- United Kingdom

Wednesday, June 12, 2019

We have previously commented on how the cyber threat to every UK pension scheme must now be very firmly at the top of every trustee's risk register. GDPR has only served to highlight a fundamental challenge to the cybersecurity of schemes, a challenge that seems to evolve and grow by the week.

PASA has just published some important guidance on cybersecurity risk and risk management to help trustees and their schemes manage the risks. That guidance covers five main areas: risk assessment, governance, risk management, controls and incident management.

Risk assessment

To carry out successful risk assessments, the guidance suggests that trustees must agree what they are trying to protect from cyber risks (e.g. member data), identify the threats, look at relevant controls in place and then assess the likely impact of the risk. They can then go on to consider risk management and the controls in place to assist with that.

Governance

The guidance cross-refers trustees to TPR governance principles and recommends that these are applied by schemes (for example, having clear responsibilities and accountabilities for cyber risk, regular training to help understand evolving cyber risks and protecting personal data and other assets with suitable controls).

Risk management

The guidance says that ownership of cyber risk management should be at board level and feature on the scheme's risk register. It will never be possible to mitigate all cyber risks, but they can be at least managed or reduced by thorough and regular reviews. Trustees should also consider what insurance they have in place that may respond in the event of a cyberattack or data breach.

Controls

The guidance urges schemes to look at organisational controls that can mitigate cybersecurity risks (whilst acknowledging that not all of them will apply to all schemes) for example:

- implementing robust and up to date (tested) business continuity/disaster recovery plans
- reviewing and, where necessary, updating data protection policies/procedures
- reviewing infrastructure to ensure that it is appropriate given the cyber risks that have been identified as potential threats to the scheme
- internal user management to keep the scheme safe from internal cyber risk threats, keeping access details (for example, log in/building access) suitable and up to date

Incident management

The guidance highlights the importance of trustees having a data breach incident response plan to support the scheme in the event of a cyber incident which includes individuals' individual and collective responsibility for addressing cyber issues.

The guidance is intended to provide practical support for trustees in formulating a robust and effective review of how they might safeguard their schemes from cybersecurity issues. Whilst inevitably it can only scratch the surface as to how trustees might confront cyber risk, it is nevertheless a useful summary of the issues that trustees and schemes must think about in this fast moving area.