SQUIRE
PATTON BOGGS

Protect Against Unmitigated Liabilities #meetPAUL #How2DoPensions

Campaign Overview

Earlier this year, we conducted a survey to assess how confident trustees and corporate sponsors felt about 10 fundamental areas of pensions risk. We focussed on areas not directly covered by the Integrated Risk Management Framework, and asked respondents to rank the risks in order of their "stay awake" factor. We have now produced a series of 10 factsheets, each one commenting on one of the survey risks. Our red risk flags highlight some key warning signs, and our mitigation tips are designed to supplement existing areas of risk mitigation. Each factsheet assumes there is an established risk management system on which additional measures can be built.

Risk 4: Data Protection Failings and Cybersecurity

Survey Result

This risk ranked fourth in our survey and it is included on 92% of risk registers. When we asked our survey respondents to provide examples of key mitigating actions undertaken by their scheme, the most common example given was the review of processes and contracts for General Data Protection Regulation (GDPR) compliance.

Comment

Pension schemes are particularly exposed to risks stemming from inadequate data protection and cybersecurity safeguards, due to the quantity of personal data that is processed and the high volume of financial transactions. A cyberattack or data breach can have severe (and costly) consequences for a pension scheme and its members. Non-compliance with the new tough GDPR standards can also result in substantial penalties.

In the lead up to May 2018, the pensions industry was consumed by GDPR compliance. As part of this, trustees will have reviewed the data protection safeguards that they and their service providers have in place. Now that the GDPR dust has settled, trustees could review the initial work that they undertook to identify any improvements, including measures that need to be revisited because of subsequent change (e.g. a change of administrator).

Cybersecurity risks are constantly evolving; therefore, safeguards should remain under review. Guidance issued by PASA and The Pensions Regulator (TPR) contain recommended steps for pension schemes to protect against cyber-risk.

Red Risk Flags

- Are there any service provider contracts that have not been reviewed for GDPR compliance (where the provider has access to scheme personal data)?
- According to PASA, the most common causes of security breaches relate to human error. Is there a process for training employees on data security – such as individuals within the payroll or pensions management teams?
- Are personal email addresses, tablets or mobile phones used for scheme correspondence or for accessing personal data? These may not be fully secure.

Mitigation Tips

- Test the scheme's procedures for dealing with, and recovering from, cyberattacks or other data breach incidents. PASA considers independent regular and effective penetration testing to be best practice to identify weaknesses.
- Do the trustees have access to IT expertise within the corporate sponsor's company, and can this expertise be drawn upon to assist with cybersecurity risk assessments and testing?
- Review trustee insurance policies to check whether they would cover the costs associated with a cyberattack or data breach.
- Timetable regular reviews of cybersecurity and data protection policies and safeguards into trustee business plans.

A Word from The Pensions Regulator

> "What about you? Trustees and scheme managers themselves receive and send large amounts of potentially sensitive information. You should ensure that you have the right controls around your own work, e.g. clear policies on what can and can't be sent to personal email addresses or accessed on tablets and mobile phones."

(From "Cyber Security Principles for Pension Schemes", April 2018)