Cyber security: is your scheme managing the risk?

By Caroline Marshall, Associate, Sackers

Research published last year by The Pensions Regulator (TPR) showed that a quarter of pension schemes had less than half of the recommended controls in place to protect their data and assets from cyber risk. Are pension schemes behind the curve when it comes to managing cyber security risks, and what steps can they take to improve?

What is cyber risk?

In a world that is increasingly reliant on digital technology, all organisations are now at heightened risk of a cyber security incident.

In the pensions context, a cyber incident can mean loss, disruption or damage to a scheme as a result of failures in IT systems and processes, posing risks to data security as well as assets. Pension schemes are a particularly lucrative target for cyber criminals, due to the large volume of member data and assets they hold. Despite this, TPR's findings suggest that schemes could be doing more when it comes to managing their risks.

TPR has been paying increasing attention to the matter of cyber security in recent years. In April 2018 it published its 'Cyber Security Principles for Pension Schemes' guidance, making clear that it expects schemes of all sizes to be alert to these issues and to take preventative action.

But although scheme trustees and administrators may be aware of the need to protect their schemes and their members, they may not feel adequately prepared in the face of cyber risks.

Be prepared: steps schemes can take now

Understand the risk

As a starting point, schemes should ensure that they understand the cyber threats they face, record the issues on a risk register and keep this under regular review. Schemes should take a holistic approach to information security, assessing all systems for potential vulnerabilities.

To identify and monitor scheme-specific risks, schemes should utilise all the information available to them. This may include data from past complaints from members and internal and external audit reports.

Schemes should then take an approach proportionate to their profile. Larger schemes may consider establishing a sub-committee focused on identifying and assessing cyber security risks.

Internal controls

Having identified key risks, schemes should take steps to address them by improving internal procedures. Particular focus should be given to procedures involving the transfer of member data. Schemes should also work with all relevant parties (including in-house functions, third party service providers and employers) to agree appropriate controls. In terms of member data security, measures to consider include:

- ensuring there are appropriate security measures in place where members have access to pension information online
- considering any additional training which service provider staff may need to ensure compliance with obligations under data protection legislation
- taking steps to monitor the security measures for staff who have access to scheme and member records.

Cyber threat is a challenge that is constantly evolving. A regular review of these measures by schemes and their service providers will improve the strength of preventative action taken.

Make a response plan

In the event that a cyber security incident takes place, schemes should have a plan pre-prepared.

An incident response plan should set out how, in what circumstances, and by whom trustees will be notified of a cyber security incident. It should cover what the scheme and the relevant third parties will do to investigate and mitigate a breach once detected, and when and how a scheme will make any necessary notifications, including to TPR, the Information Commissioner's Office (ICO) and scheme members, where relevant.

Establish a recovery plan

'Cyber resilience' is not only a scheme's ability to prevent incidents from taking place, but its ability to recover if the worst happens. This may include arranging back-up data systems and a plan for contacting members in order to manage reputational risk to the scheme.

Investigate any incidents

Schemes should ensure that any incidents that do happen are fully investigated and records are kept of the cause and effect. This gives the opportunity to identify weaknesses in processes, so that they can be remedied, and in turn help to prevent future incidents.

Educate your members

Some pension scheme members may be particularly vulnerable cyber crime targets. Once schemes identify the risks faced, they should ensure that members are given the right information in order to try to help them identify when they are the target of potential scams and cyber threats. Schemes can do this by including information on cyber security in member communications, and, for example, regularly reminding members of how the scheme administrator would make legitimate contact with them.

Schedule trustee training

Last year, the Pensions Administration Standards Association (PASA) published cyber security guidance aimed at providing practical support for trustees. This guidance identified human error as the most common cause of cyber security incidents.

It's not uncommon for trustees to have access to scheme data at home or on the go, or to conduct scheme business using a personal email address.

By ensuring trustees are regularly trained on developments in industry standards and how to identify cyber security threats, schemes can be proactive towards managing the risk of an incident.

Whilst no degree of planning can prevent an attempt, sensible steps can help prepare for, control, and mitigate an attack.