HYMANS # ROBERTSON

Sixty second summary

Cyber risk in the LGPS

With significant cyber breaches hitting the headlines almost daily and the Pensions Regulator's growing expectations, cyber risk has become an increasingly topical issue for the LGPS. In such a busy time for funds, you need to focus on the right areas to improve cyber resilience.

Understanding the importance of cyber-crime

Even before the pandemic hit, the fact that we were living in a far more connected world, with data being shared between organisations and services increasingly moving online, meant the threat of a cyber attack was already significant. Add the impact of homeworking into the mix and it only serves to increase the potential threat from cyber criminals.

And you don't need to look too hard in the media these days to see the disruption cyber attacks can cause. Newsfeeds regularly highlight the latest ransomware attacks, denial of service, phishing or "zero-day" attacks. All these run the risk of loss of member data, financial loss, disruption to service and reputational damage to organisations. And public sector organisations have not been immune from the threat – in fact, they are often seen as a prime target. LGA helpfully provide some interesting case studies of the impact across local government[1] as a useful reference to cyber breaches on Councils.

Why is the LGPS potentially exposed?

Fundamentally, all LGPS funds hold large amounts of exploitable personal data and assets which are a prime target for fraudsters, scammers and cyber criminals. Funds also work with a wide range of providers and suppliers that handle their sensitive data (e.g. employers, AVC providers, software providers, actuaries, etc).

Add to this the perception and track record of the public sector having weak cyber resilience, and the reality is 'when, not if' a major cyber breach will happen to an LGPS fund.

But isn't my Fund covered by the host council's cyber support and policies?

This may well be the case, but how specifically does it cover fund risks? How well do the Council's IT and Business Continuity teams know the fund's systems, users, stakeholders, suppliers, etc? If there was a cyber attack on the Host Council's systems which impacted the fund, how much priority would the fund receive during the attack and in recovery? What are the roles and responsibilities of Fund officers and committee/board members?

[1] Case studies | Local Government Association

The Pensions Regulator (TPR) is very clear that a fund shouldn't solely rely on the Host Council's cyber policies and procedures. Its special guidance expects steps to be taken to build up cyber resilience (i.e. minimising the risk of a cyber incident occurring and recovering if an incident does occur) through an assessment cycle:

Assess and understand risks – put controls in place – monitor and report

Assessing the impact of cyber-security risks should, therefore, be owned by Fund officers and committee and board members, with cyber risk featuring on Fund risk registers, as well as becoming a regular feature on committee and board agendas.

What should funds do?

If not already being implemented, steps should be taken to build up the cyber resilience of the Fund and ensure strong governance around the risks. Key priorities should include:

- Undertaking training, in order to gain an understanding of the Fund's cyber security approach and recovery plan;
- Understanding the reach of the Fund's cyber footprint, including collaboration with external partners;
- Engaging with the host council to understand current cyber security arrangements and how the Fund fits into these;
- Reviewing the Fund's governance arrangements and polices to incorporate the evolving cyber risk; and
- Ensuring the administration function has a robust business continuity/incidence response plan in place which is known to key officers and committee members;

How can Hymans help?

We don't believe the housekeeping needed to get up-to-speed on cyber risk means large amounts of work or cost. Our view is that the best approach is to be targeted and proportionate – focusing initially on the governance of cyber risk. With that in mind, we suggest arranging initial support in two key areas:

1. Officer and Committee/Board training session – comprising a 1.5h foundation session covering the key cyber security risks faced by LGPS funds:

- Why pension schemes are targeted?
- Details of specific cyber risks faced by funds and the consequences of cyber incidents
- LGPS roles and responsibilities on cyber risk
- TPR's perspective and expectations
- How cyber resilience can be achieved (including discussion on the link to host authority policies and procedures)

2. Policy development and integration - assist you to develop a Fund-specific cyber security policy - importantly, (i) integrating cyber risk into the Fund's current governance and risk management structure and (ii) complimenting the host authority's corporate cyber policies and strategies.

Following this groundwork, we are also happy to provide further assistance e.g. mapping the fund's cyber footprint, scenarios workshops, incident response plan support, etc.

Conclusion

Given the significant risks and implications on LGPS funds of a cyber attack, it is vital that resilience and strong governance is built into the culture of your Fund and registers high on your list of priorities. If you would like to discuss this matter further, then please feel free to get in touch with your usual Hymans contact.