BARNETT WADDINGHAM
beyond the expected

Cyber Security for Pension Schemes

In an age where technology plays such a huge part in everyday life, nobody is immune to the risks posed by cyber threats. Pension schemes are no exception to this and both trustees and pension managers need to take active steps to protect members and assets against cyber risk.

So what is cyber risk?

Put simply, cyber risk is the risk of a financial loss, disruption or reputational damage from a failure of information technology systems or processes. Cyber security is about protecting computers and infrastructure from cyber risk. Cyber risks can come from a variety of sources, including external targeted attacks such as malware or ransomware, internal risks from either accidental or deliberate means, or a breach in the supplier chain.

As potential security risks grow in volume and sophistication, The Pensions Regulator sets out that trustees should have in place a robust and effective plan of action in case the worst unfortunately happens.

> "The cyber risk is complex and evolving, and requires a dynamic response. Your controls, processes and response plan should be regularly tested and reviewed."
>
> The Pensions Regulator

Building cyber security resilience

So just how do trustees minimise the risk of an incident occurring? Surely there is not much that can be done?

Well actually, many things can be done. They range from removing or disabling unnecessary functionality from systems through to establishing risk policies and procedures for home and mobile working.

The Pension Administration Standards Association (PASA) has issued guidance to provide practical cyber security support to trustees.

Trustees should work through a process of understanding the risks and the assets they are trying to protect. Once these have been established, trustees can look to analyse the impact versus the likelihood of an incident by using their trustees' risk register.

Controls should be put in place to mitigate the identified risks, including checking the cyber policies and controls in place at third party suppliers. Once in place, controls should be monitored and reviewed regularly so that they can evolve in response to changes in the fast-moving cyber landscape.

And what if the worst should happen?

Trustees should have in place a Cyber Security Incident Response Plan that they understand and regularly review, just in case the worst happens. Trustees need to respond to an incident swiftly and in the right way. Would you know how to react?

How do you get ready?

We can help by:

- providing training on the governance of cyber security
- helping you to understand the risks and capture them on your risk register
- developing and maintaining your cyber security controls and monitoring compliance with them
- developing and maintaining your Incident Response Plan.

Please contact your Barnett Waddingham consultant if you would like to discuss any of the above topics in more detail. Alternatively get in touch via the following:

info@barnett-waddingham.co.uk 0333 11 11 222

www.barnett-waddingham.co.uk