Trafalgar House

Trustees opening themselves up to cyber risks if they don't respond to NCSC reporting changes, says Trafalgar House

Press release: 06 02 2024

Trafalgar House, a specialist third-party pensions administrator, today urged schemes to ensure they, and their advisors, review their cyber incident monitoring and reporting frameworks in light of the changes to weekly threat reporting that have been made by the National Cyber Security Centre (NCSC). A change at the end of last year in the reporting framework from the NCSC has meant that threat and incident analysis is no longer available from their usual reporting sources.

Stephen Wright, Head of IT, said: "The change in NCSC threat reporting frameworks, which came into effect at the end last year, significantly alter the way advisories are issued and reported. Cybersecurity has fast become one of the biggest threats to schemes. Data breeches, scamming, ransomware, fraud - these have all become the stuff of trustee nightmares. And the sophistication of those threats is evolving rapidly, so it is important that schemes stay as far ahead of them as possible with comprehensive and proactive defense measures. It's also imperative to check-in regularly with advisors that their measures are robust, and reports are undertaken frequently to demonstrate progression of mitigation of all vulnerabilities. A onetime spot check is simply not enough in this environment.

"There are some immediate actions schemes could, and should, take:

- **Verify cyber threat analysis updates:** Confirm that all your advisers are proactively updating and refining their cyber threat analysis reports. It's crucial that they regularly review and enhance their threat intelligence capabilities to protect against evolving cyber threats.
- **Enquire about intelligence sharing participation:** Directly question your advisers on their involvement with intelligence sharing networks, such as the Cyber Information Sharing Partnership (CiSP). Participation in such frameworks is essential for staying informed about imminent threats and adopting best-practice responses.
- **Clarify threat identification and management:** Gain a clear understanding of the mechanisms your advisers use to detect relevant cyber threats and incidents. Request detailed explanations on how these are integrated into their active risk management processes, ensuring a robust defence mechanism is in place.
- **Demand comprehensive and ongoing threat reporting**: Insist on receiving frequent, detailed reports covering the spectrum of threat management activities—highlighting ongoing, resolved, and

potential threats. These reports should demonstrate a continuous commitment to cyber security, reflecting an adaptive and responsive strategy to evolving cyber threats.

- **Check the procedures your advisors have in place** – are they robust enough? Are they being constantly evaluated and updated?! What are vulnerability scores? Do they adequately protect their business and client data?"

Wright added: "Sadly, the issue of cyber security isn't going anywhere but the good news is there is a lot that schemes can do to stay ahead of the curve and protect members."

(ENDS)

Notes to editors:

Trafalgar House is a specialist pensions administrator.

Founded in 2006, our mission is to set the highest standard of pensions administration by any recognised measure. We achieve this through sustained investment in our people, processes, and systems.

We started life as an in-house administrator. Our foundations are in quality and member experience. Since our creation, we have grown as a third-party administrator. Adopting technology and innovation from across the market, we have emerged as a business of administration experts.

We have offices in London and Farnborough, over 30 clients and 160 staff. We hold internationally recognised accreditations for quality, security, development, customer service and environmental protection.

Media Contact:

For all media enquiries please contact KBPR using the details below:

kate@kbpr.agency | 07930 442 883