Always on: Cyber incident planning

Aon associate partner, John Harney, looks at why cyber incident response planning for pension schemes must be an ongoing strategic priority – not a 'one and done' exercise

We are all aware of the ever-evolving nature of cyber threats to organisations, including pension schemes.

Cyber risk is an increasingly pervasive real-world threat and The Pensions Regulator (TPR) has published detailed guidance for trustees, which includes expectations around incident response planning. Simply put, a scheme's incident response plan should not consist of letting providers and the sponsor manage the incident as best they can. Trustees play a crucial role in overseeing how the scheme responds to cyber incidents, which should also be considered a risk event when completing their Own Risk Assessment.

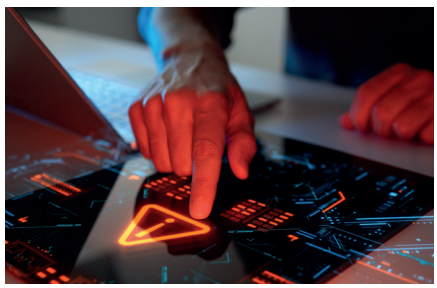
Wider practice

Beyond the UK, the EU's Digital Operational Resilience Act (DORA) sets out clear standards for pension schemes by classifying them as financial institutions, highlighting their importance in providing retirement income. Given the risk of outages – whether accidental or malicious – operational resilience and maintaining critical functions like regular pension payments are essential.

The centrepiece of this legislation is a requirement for schemes to be prepared for incidents, including putting in place, reporting major cyber incidents within four hours and regularly testing an incident response plan.

Regular scenario testing

Many UK pension schemes have carried out scenario testing over the past few years, however, response plans must keep



pace with evolving cyber threats and changes to the scheme's governance and operational structure. For example, after a buy-in does your incident response plan still meet current needs?

As well as refining existing incident response plans, these scenario testing sessions (sometimes referred to as 'wargames') are helpful training for trustee boards on cyber risk more generally and what it means for their specific scheme's processes and operations.

Testing sessions can be held with different focuses. This can be achieved by considering various scenarios, but also by inviting key providers to participate alongside the trustees. Alternatively, the session might focus specially on operational, member or financial impacts of a cyber incident.

As well as deep-dive exercises on a biennial or triennial basis, schemes can also carry out abridged, annual testing. This is already a requirement for EU-based schemes under DORA.

Response planning, including the creation of a testing plan, is not solely a legal matter. It requires risk management while considering relevant legal obligations to members and regulators. It is also not just a question of data security. Assets can be at risk, as well as the overall operations of the scheme and day-to-day member services. Appropriate planning also involves developing a communication strategy so trustees know 'how' as well as 'what' they would want to tell members in the event of an incident.

Cyber incidents and overall scheme strategy

In 2025, pension schemes must consider more stakeholders, like buy-in providers and dashboards. There is a serious risk that a cyber incident could disrupt large projects, endgame planning, transaction preparation, or, indeed, dashboards connections. Running suitable test sessions can reduce the wider impact of such incidents on scheme priorities.

Another outcome from testing sessions is a clearer view on proactive steps to take to manage operational and cyber risk. For example, establishing a more structured approach to the depth and regularity of assessments of third-party providers or getting a clear picture of the scheme's cyber footprint through a data and asset map.

Trustee leadership

Trustees are ultimately responsible in the event of an incident and they should set the pace and coordinate the response, even if they are reliant on third parties for information or support. They should be looking ahead, to ensure everyone is coordinated, moving at the right pace and staying together. In the same way, scheme trustees should be thinking ahead to what might be coming next, and regularly testing their incident response plan will help them in doing so.

Written by Aon associate partner, John Harney