fieldfisher

Cyber Risk Radar for Pension Schemes

Providing Members the access they want Regulatory action Like everyone, pension scheme members use If an attack shows poor internal controls or a failure to review them the Trustees may be penalised by the mobile and instant technology to access information and services and, increasingly, to Pensions Regulator. A cyber attack resulting in data effect transactions. The market is increasingly loss will almost certainly produce a regulatory providing phone apps for benefits statements, investigation if it becomes known and possible web portals for retirement planning and for enforcement action (which may include a fine) from storing, checking and updating personal details. the Information Commissioner. **Contractual terms Duty to have Internal Controls** Do the trustees' contracts with their Trustees must establish and administrator and service provider allocate operate a system of internal risk for cyber security clearly and controls which are adequate for appropriately? Do they provide for reviews securing compliance with all laws. to align with the internal controls duty on **Cyber Criminals** trustees? Do they comply with information Criminals look for weaknesses security law and regulatory expectations? and migrate to where they see **Member Claims** weakness. Cyber criminals do the If a member loses financially or is otherwise same but with more speed, less harmed through loss of data they are likely to visibility and powerful claim against the Trustees. But even if there technology. There is a range of is no loss of data, there may be claimable threats - external hackers for harm because of the stress of taking profit, campaigning "hacktivists", additional security steps and/or changing disgruntled employees or expasswords for other accounts. employees. **Reputational Damage Information Security** The loss of personal data is a hot topic for the media and Trustees must ensure that the personal data they reputational damage always follows a serious data loss. Breach hold is kept secure and confidential at all times, in transit and at rest, whether held by them or by notification requirements or regulatory expectations may apply their service providers and data processors. They Depending on the media approach this may affect the employer must ensure appropriate due diligence, contract and the scheme's administrators. Clear positions on breach notification and a good PR strategy may determine how a breach terms, technical and organisational security measures, as well as regular audits and reviews. will be remembered.