Cyberattacks and pension schemes: understanding the risks and guidance

By Alan Cronin
October 3, 2023 |

Data protection, Pensions

Introduction

According to the Cyber security breaches survey 2023 published by the Department for Science, Innovation & Technology on 19 April 2023, 32% of businesses suffered from a cyber breach or attack in the last 12 months. This figure is higher at 69% for large businesses. Further research indicates that UK pension schemes had the biggest increase, reporting a 4,000% rise in data breach reports to the Information Commissioner's Office, going up from six in 2021/22 to 246 in 2022/23. These statistics make it clear that cyberattacks remain a key business risk across all sectors, with the pensions industry being no exception.

Due to their holding of substantial amounts of personal and sensitive data, pension schemes are key targets for these attacks. The consequences of successful cyberattacks on pension schemes can be severe, causing reputational damage for providers and financial losses for members. Such incidents could also trigger legal action from members and expose providers to considerable regulatory fines under certain serious breach circumstances. The Information Commissioner's Office (**ICO**) in particular has the power to impose fines of up to £17.5 million or the equivalent of up to 4% of annual turnover – whichever value is higher.

This growing threat makes it clear that there is a need for robust security measures within pension schemes, and therefore trustees and scheme managers need to take steps to protect their members from such attacks.

In this piece, we investigate the cybersecurity threats facing the UK's pensions sector and discuss what steps trustees could take to protect their members and assets against this risk. We also delve into the practical guidance issued by regulatory bodies such as the Pensions Regulator (**TPR**) aimed at safeguarding these crucial retirement funds against cyber threats.

Types of cyber threats for pension schemes

Pension schemes face substantial threats from various forms of cyberattacks, with phishing and ransomware attacks being of the most concern.

Phishing attacks involve scammers deceiving individuals into divulging confidential information. This has the potential to be incredibly harmful to pension schemes as, if such information is provided, it may lead to attackers gaining access to the account details of the pension scheme, where they could potentially redirect funds or make unauthorised withdrawals. It can also be problematic for the scheme provider, as a successful phishing attack has the potential to damage their reputation and make it difficult to attract new members.

Ransomware attacks are when an attacker can lock out access to critical systems until a ransom is paid. This is often done by the attacker deploying malicious software that can infiltrate and encrypt data on the network. The attacker will usually ask for this ransom to be paid in cryptocurrency, which is harder to trace and, in return, they will provide the decryption key. If this key is not provided, it may mean that this information is permanently lost.

Current regulatory landscape and guidance

As mentioned above, the financial losses for stakeholders, reputational damage for scheme providers and potential regulatory penalties due to non-compliance with data protection laws make it clear that trustees and scheme providers should prioritise cybersecurity.

TPR has set out its expectations for trustees in a new draft single code of practice. Whilst this code is not yet in force and is an early version drafted for the purpose of using within the new code of practice consultation, it echoes the points made earlier by TPR in its guidance on cyber security for pension schemes, published in April 2018.

In this draft code, TPR makes it clear that trustees and scheme managers are accountable for the security of scheme information and assets, and are required by law to operate adequate internal controls to run their scheme.

As such, steps should be taken to build up cyber resilience. TPR has set out measures that trustees should consider when (i) assessing cyber risks and (ii) managing cyber risks. These can be summarised below:

Assessing cyber risk

- *Knowledge and understanding*: The trustees should understand the cyber risks associated with their scheme.
- *Confidentiality and integrity*: Trustees should recognise the need for maintaining confidentiality, integrity and availability of systems that process personal data.
- *Defined roles and responsibilities*: Clear roles should be defined amongst providers for identifying cyber risks and breaches, as well as responding to incidents.
- *Risk register maintenance*: Cyber risk should be part of the risk register and reviewed regularly.
- *Vulnerability assessment*: Regular assessments of vulnerability to

cyber incidents should be conducted on the scheme's key functions, systems, assets (including data) and service providers.

- *Specialist skills access*: Trustees should consider bringing in specialist expertise to understand and manage these risks effectively.
- *System controls update*: Ensure that system controls such as firewalls and anti-virus software are up to date.

Managing cyber risk

- *Regular backups*: Make sure critical systems and data are backed up regularly.
- *Device usage policies*: Establish rules for device use, including home and mobile working scenarios.
- *Data policies and controls*: Implement policies controlling data access, protection, usage and transmission aligned with applicable data protection laws.
- *Policy effectiveness*: Take necessary steps to ensure these policies remain effective over time.
- *Breach reporting*: Have guidelines determining when breaches need reporting to the ICO.
- *Incident response plan*: Maintain a plan outlining steps taken during any incident ensuring operations can resume safely and swiftly – learn more at "Continuity Planning".
- *Service providers' controls evaluation*: Ensure service providers involved in running schemes have robust cybersecurity measures in place.
- *Regular reports receipt*: Receive periodic reports from staff/service providers about any identified risks or incidents that have occurred.

By following this guidance, pension schemes can significantly reduce their exposure towards potential cyber threats, overall ensuring better protection for members' interests against an evolving digital threat landscape.

As well as the above, TPR has made it clear that governing bodies should also be aware of their responsibilities under the UK General Data Protection Regulation (**GDPR**). The ICO enforces the GDPR and stipulates that scheme providers have certain obligations to report data breaches within 72 hours of them becoming aware of any breaches in personal data.

Conclusion

In the ever-evolving landscape of cyber threats, vigilance is important, especially within the pensions industry that safeguards not just significant financial assets but also vast amounts of sensitive personal data. It is therefore crucial for trustees and scheme providers to keep abreast of latest cybersecurity trends and potential vulnerabilities – they should ensure that they keep up to date with regulatory guidance to build their cyber resilience and

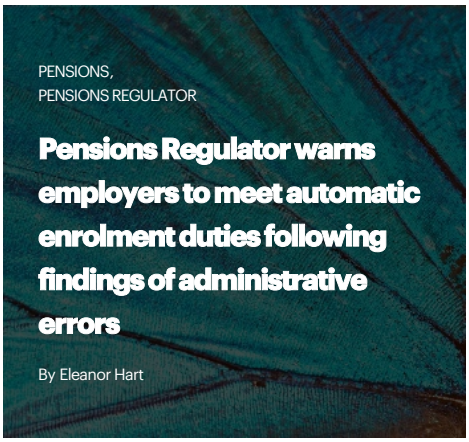
assess their approach to risk management policies.

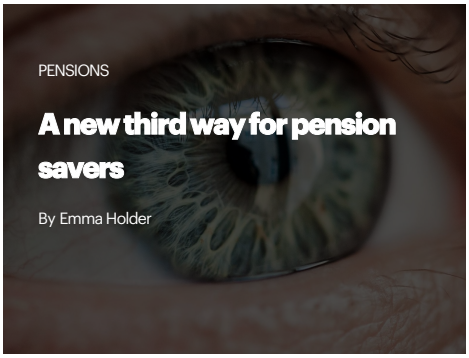
Data Protection, Pensions

About Alan Cronin

ALL POSTS

You might also like...





DATA PROTECTION,
DISCRIMINATION,
EMPLOYMENT CONTRACTS

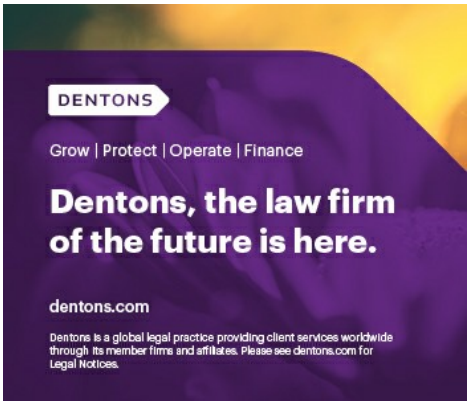
Philosophical belief case on right to copyright fails

Is an argument about the interpretation of a contract protected as a philosophical belief? No, said the Court of Appeal [...]

By Aggie Salt

About Dentons

Across over 80 countries, Dentons helps you grow, protect, operate and finance your organization by providing uniquely global and deeply local legal solutions. Polycentric, purpose-driven and committed to inclusion, diversity, equity and sustainability, we focus on what matters most to you. www.dentons.com



Categories

Select Category

DENTONS