How to stay one step ahead of the hackers

The pensions industry is a key target for cyber criminals, so what can providers do to protect themselves and what should they do if they fall victim to a data breach?

Summary
- Cyber criminals are constantly evolving techniques to gain access to data.
- TPR requires pension schemes to plan measures for a possible breach.
- Best practice is to maintain a well-prepared and tested incident response plan.
- Pension schemes need to regularly review and update their processes.

Pension providers hold huge amounts of valuable data, making them a prime target for criminal hackers seeking to access members' personal information. Several recent major data breaches have left the industry reeling, with many providers looking to protect themselves from a similar cyber attack.

Pension schemes and administrators hold key data, including members' names, addresses, national insurance numbers and even bank details, when the provider is paying out a pension. Data can be stored, handled and shared by various parties – including external third parties from communications consultants to independent financial advisers (IFAs) – as part of the normal running of a pension scheme.

Schemes and administrators are also particularly vulnerable to ransom requests. If a provider chooses not to pay the ransom, the stolen data can be sold on the dark web, leaving members vulnerable to identity theft. In addition, due to many members' reliance of receiving their pensions on time, the provider is under pressure to resolve the issue quickly so it can regain control of its data and resume its operations.

Time pressure

Time is a key factor when a provider's data is breached. Once providers notify

a scheme's trustees that there has been a breach, they have 72 hours to inform the Information Commissioners Office (ICO).

"Cyber criminals are becoming increasingly sophisticated and the forms of attack are evolving all the time. We should accept that the pensions industry is a digital one and cyber risk is a very real threat," says Mercer senior principal, governance leader, Lindsay Sadler.

On the other hand, one of the benefits of the industry's digitalisation is that re-mobilising after a data breach has become a smoother process. Capital Cranfield professional trustee, Paul Watson, was working with a provider that was impacted by a data breach but was able to react to it quickly, partly thanks to the increasingly digital interconnections within the industry.

"We had a cyber policy in place and, as documented, we quickly mobilised the sub-group to consider the issue and the appropriate actions," he says. "One challenging feature we hadn't considered previously, in our preparations and policies, was the impact of such an event being across many schemes of the same provider at the same time."

The provider had limited resources available to support the board due to the requirements of the various schemes. "One reassuring aspect was the quality of the advisers we had in place – the individuals taking ownership and responsibility as well as the wider support of their firm. You don't always appreciate the value of an adviser until you're up against it. Although, naturally, it came at a considerable cost," he says.

Lessons for the sector

A pension scheme will never be completely immune to the risk of a cyber-security attack, particularly when cyber criminals are becoming increasingly sophisticated, and the forms of their attacks are constantly evolving. However, steps can be taken to mitigate the risk a breach poses and reassure members.

"We advocate an approach where pension scheme trustees and managers educate themselves on the threats and nature of cyber risk by undertaking training with cyber-risk experts, helping them understand their roles and responsibilities and prepare them to handle the difficult decisions they will face during an attack," Sadler says.

"Pensions knowledge does not equate to cyber knowledge and therefore this training should not be undertaken by pension advisers. This training should be specific to the pension scheme and its

Examples of security breaches within the pensions sector

In April 2023, Capita said that it had experienced a cyber incident and that there was evidence of "limited data exfiltration from the small proportion of affected service estate that might include some customer, supplier or colleague data".

The Pensions Regulator later revealed that it had written to pension schemes that use Capita as their administrator, asking trustees to speak to Capita as to whether there was a risk to scheme data, with the Financial Conduct Authority also engaging with the provider.

A number of pension schemes and providers, including the M&S Pension Scheme and Universities Superannuation Scheme, wrote to members to confirm they were impacted by the breach.

Capita revealed in May that it expected to spend between £15-£20 million in relation to the cyber incident, including specialist professional fees, recovery and remediation costs and investment to reinforce its cyber security.

A spokesperson for Capita said: "Capita continues to work closely with specialist advisers and forensic experts to investigate the incident and we have taken extensive steps to recover and secure the data.

"In line with our previous announcement, we are now informing those we have identified to be affected.

"We are working to provide our clients and their customers with information, reassurance and support while delivering for them as a business. In instances where we need to provide further support to those affected, we will do so."

Meanwhile, The Pensions Ombudsman (TPO) revealed in June that it had temporarily disabled some systems as a precautionary measure while it worked to investigate a cyber incident, with members instead told to get in touch via the ombudsman's phone lines or email options.

TPO confirmed that it has been working with the relevant agencies, including the National Cyber Security Centre, to respond to this cyber incident.

TPO stated: "As a precautionary measure, access to some systems was disabled which temporarily impacted on our ability to deliver services and manage enquiries from the public.

"Our priority has been to restore services securely and safely and we are pleased to confirm that services have been restored.

"There may be some service delays while we work through recent enquiries and applications. We apologise for any inconvenience."

In light of the potential delays expected, however, the ombudsman also confirmed that, wherever possible, it will use its discretion to expand the time limits for new applicants affected if it has not allowed them to apply within the legislative limits.

nuances, such as which third parties it works with and whether they outsource administration functions."

The pensions industry is very aware of the fact that it might be the target of data breaches, according to Eversheds Sutherland partner, Emma King. "Firms have been revisiting their contracts with suppliers and providers to ensure they are as watertight as possible, and looking at what recourse they have in the case of something going wrong. They've also looked at the protocols they have in place in the case of a breach and what steps need to be taken."

The Pensions Regulator (TPR) has set out its expectations for pension scheme trustees. In its new General Code, it states that for pension schemes to have an effective system of governance, its internal controls need to include measures that reduce cyber risk. It also states that functioning cyber controls will help trustees comply with data protection legislation and may reduce its liabilities in the event of a data breach.

Finbourne co-founder and head of platform engineering, Chris Brook, advises schemes to assess their business systems to ensure they remain protected.

"All business systems require constant maintenance and enhancement to remain protected against evolving security threats, and legacy or out-of-date technology platforms can present an easier target for attackers," he says. "Modern cloud-native SaaS solutions can offer very strong security protections, by building upon highly secure cloud infrastructure, and by harnessing economies of scale to provide cutting-edge security countermeasures that may not be commercially viable for self-hosted systems."

"We should accept that the pensions industry is a digital one and cyber risk is a very real threat"

However, Sadler points out that human error is the cause of the vast majority of cyber incidents. "The people who form part of the pensions ecosystem also need to ensure they are acting in a cyber secure way and are vigilant to their own working practices, such as the use of public wi-fi or personal devices. A cyber policy helps with this by setting out how third parties will be assessed and how the pension scheme trustees are expected to behave when interacting with scheme data," she says.

Forward planning

Breaches can have a devastating impact on the reputation and brand perception of pension schemes, their trustee boards and their parent companies. A proactive response to a breach is the best course of action for victims of cyber criminals.

Informing the ICO and TPR about a breach of personal data requires the scheme's designated data protection officer to have a very clear understanding of the guidance set out by the regulator. If not handled correctly, it could end up causing significant damage from a financial and reputational perspective. Therefore, undergoing crisis training is crucial.

"Having a well prepared and tested incident response plan would greatly reduce the impacts of an incident," Sadler says. "A good plan will set out the roles and responsibilities of the team who will be responsible for responding to the incident as well as the practical steps to deal with impacts, including the communications strategy both internally to impacted colleagues and externally to members of the scheme."

"Due to the evolving nature of cyber threats, protecting yourself from these isn't a 'one and done' exercise. We recommend regular training and review of policies and procedures to ensure these are kept up to date with the nature of the risk," she adds.

Large scale breaches have meant that trustees and members remain worried about the threat of a cyber-security attack.

"Our experience left us with a lot to reflect on as a trustee board and for our members it was, and remains, a very worrying period. The trustees may have legally met their obligations, but it was a highly uncomfortable experience for members that we are acutely aware of," Watson says.

Eversheds Sutherland global cyber security and data privacy team legal director, Lorna Doggett, recommends a three-pronged approach to preparing for a data breach.

"You need to do your due diligence, training, and have the governance documents and policies around cyber-security. In line with TPR's guidance, schemes should set out how they are ready for cyber risks," she says.

Written by Beth Ure, a freelance journalist