NORTON ROSE FULBRIGHT

UK Pensions Briefing

Taking action on pension scheme cybersecurity

August 2021

Introduction

Cybercrime is continuing to grow and pension schemes are attractive targets for cybercriminals. Ransomware is currently the biggest cybersecurity threat to schemes but few schemes are adequately prepared for a cyberattack. We look at protecting your scheme – understanding your footprint, developing a cyber incident response plan and adopting appropriate cybersecurity practices.

A growing problem

Cybercrime is continuing to grow in scale and complexity. UK Government figures from 2021 show that roughly four in ten UK businesses had experienced a cyberattack or cybersecurity breach in the last year. Those falling victim include sophisticated targets. A recent example involved hackers exploiting weaknesses in a widely-used file transfer programme, giving them access to data of multiple high-profile corporate entities including an international law firm, a major US supermarket and a well-known investment bank.

The Pensions Regulator sees cybersecurity as a "pressing issue" for pension schemes and has recently included new expectations for trustees in its draft single code of practice. The Pensions Regulator wants to see trustees properly addressing the very real cyber risk to their schemes.

Why is cybersecurity so important?

Pension schemes are attractive targets for cybercriminals because:

- They hold large volumes of valuable and sensitive personal data.
- It is critical that they can make regular payments to pensioners without disruption and this makes them vulnerable to ransom demands.

The problem is compounded by the fact that many schemes are underprepared for a cyberattack. A recent Aon survey found that fewer than one in five schemes had clearly documented "cyber hygiene" policies, and only 40% stated that they had a robust incident response plan in place. Pension schemes are probably relatively soft targets for cybercriminals as a result.

Meanwhile, the regulatory landscape is becoming harsher, particularly with respect to data breaches (a common outcome of successful cyberattacks). Regulatory fines for breaches of data protection laws rose by almost 40% across Europe in 2020-2021. Fines from the UK Information Commissioner's Office (ICO) have run into tens of millions of pounds in some recent cases.

Data breach litigation is also growing. Both individual and group actions may be brought against data controllers.

In addition to these legal risks, a high-profile cyberattack has the potential to cause significant reputational damage both to the scheme and to the sponsoring employer group. This effect may be less easy to quantify; however, it may also be more difficult to remedy. No scheme member likes the idea of their personal and financial information being insecure.

What are the main cybersecurity threats?

Ransomware is currently the biggest cybersecurity threat to pension schemes.

A typical ransomware attack involves an attacker gaining access to a corporate network (often via an initial phishing attack) and deploying a type of malicious software which encrypts data on the network. Typically this is accompanied by exfiltration of files and data from the victim company's network. The attacker may demand a ransom payment – usually in cryptocurrencies such as Bitcoin or Monero – in exchange for the data to be decrypted and for stolen data to be safely deleted.

If the ransom is not paid, the attackers will not provide a decryption key, which can render some data permanently inaccessible and can necessitate reliance on backups. Worse still, attackers may also leak data stolen from the network online if the ransom is not paid. Paying a ransom, while not illegal, needs careful consideration from the point of view of compliance with international sanctions and counter-terrorism legislation.

Remember, you don't need data to be publicly released for a cybersecurity incident to amount to a personal data breach under data protection laws. Even if an attacker merely gains access to personal data it constitutes a data breach. That can trigger reporting obligations to the ICO and potentially to the Pensions Regulator and scheme members.

What does this mean for scheme trustees?

Statement of the obvious, but you can be liable for failure to manage cyber risk. As highlighted by the Pensions Regulator's cybersecurity guidance, trustees continue to be ultimately accountable for the security of scheme information and assets even where you delegate or outsource the day-to-day functions of your scheme to external administrators. That means cybersecurity is fundamental to your legal duties to ensure effective scheme governance, to protect members' personal data and scheme assets and to pay benefits.

What steps do trustees need to take?

Engagement with administrators and other third parties

You need to understand your scheme's "cyber footprint". The footprint is the extent of the digital presence of all parties involved in the scheme and the risks they pose. Then check that all third party suppliers – and in particular any external administrator – have put sufficient controls in place.

Action points:

- Actively consider cybersecurity when procuring any new services or reviewing existing providers – what do your existing administration agreements say?
- Regularly review your service providers' cybersecurity policies and controls against industry best practice.
- Understand how and when your service providers would inform you of a cyber incident – make sure you are getting regular reports from them on cyber risks.

For each of the above, think about what help you need to make sure you are protecting your scheme appropriately. Does your sponsoring employer's group have internal cybersecurity expertise you could draw on? If not, consider getting external expertise in to help you understand and manage the risks.

Cyber incident response plan and risk register

Do you have a cyber incident response plan in place? You have probably already added cyber risk to your scheme's risk register for regular review, but how far have you thought through what you would do if a cyberattack actually happened? You need to be ready to respond rapidly to a cyberattack and meet any urgent deadlines, such as ICO notification time limits. As part of your incident response planning, think about pre-agreeing terms of engagement with thirdparty experts (including cyber-forensics experts, PR/communications teams and/or specialist legal counsel) so that you can hit the ground running.

Written policies

Think about how you are mitigating the risk. Do you have written policies on areas such as:

- The acceptable use of personal devices, email and the internet (including social media).
- The use of passwords.
- Home and mobile working.
- Data access, protection (including encryption), use and transmission?

If not, now's the time to work them up and put them into practice. These are all areas where setting up the ground rules from the start, and keeping them under review, will help reduce your risk. They will also help you defend against a claim that you were not adequately protecting the scheme.

Back-ups, monitoring and logging

To assess and recover from a cyber incident effectively you need good data back-ups, monitoring and logging. The Pensions Regulator's cybersecurity guidance recommends:

- Regularly backing up critical systems and data (including, if appropriate, by way of offline back-ups to avoid them being affected in a cyber incident).
- Monitoring the network and analysing logging history to check for suspicious activity or access.

Appropriate monitoring, including the use of technical tools such as endpoint detection and response (EDR) software, is critical. Many regulators now expect organisations to be doing this as a cybersecurity minimum.

This is something your administrator should be doing for you, but make sure you understand what they are doing and what they would do, and in what time scale, if any discrepancies did show up.

To fulfil your data protection obligations, make sure you understand and assess what technical and organisational measures are in place as a whole. Are they appropriate to protect your scheme?

Information governance

The question of data retention is a tricky one for pension schemes. On the one hand we all know that claims can come in many years after a member has transferred out and that retaining a full data set for a member is the only way to be able to check calculations if a problem comes up later.

On the other hand, data protection requirements focus on not over-retaining data. Many recent incidents have involved breaches of data which the victim organisation should not have been holding at the time of the incident (including, in some cases, in violation of the organisation's own data retention policies). There have been a number of recent fines in this area.

That means being clear in your data retention policy what data should be retained, in what form, for how long, and why. It's an area where legal advice can really help .

Cyber insurance

Cybersecurity insurance exists and can provide some unique policy features, such as immediate access to legal, forensic and PR/communications external service providers. That said, policy terms and coverage will vary from insurer to insurer. If your organisation has not already invested in cyber insurance, the first thing to do is to check whether your existing insurance policies (e.g. pension trustee liability (PTL) insurance) already provide some protection and to consider how cyber insurance might supplement this.

Trouble closer to home

Trustees and the employers' pension team may regularly receive sensitive information about scheme members. "Cyber hygiene" starts at home. How clear are you on how trustees/trustee directors should access and hold that information? Think about having clear policies on how the core trustee team stores and shares information, with the right controls in place, e.g. clear policies on what can and cannot be sent to personal email addresses, printed, or accessed via mobile devices.

Trustee training

Last but not least, cybersecurity is a rapidly developing, complex area. Cyber risks are constantly evolving, and cybersecurity measures will need to evolve with changes in the legal and cyber landscape. That means setting up regular training cycles to stay on top of what's needed.

There are two things to focus on here, combatting complacency, and embedding an understanding of how to swing into action in a cyber-related emergency. Would it help to get a provider to run simulation exercises such as mock phishing emails for the trustee team and their administrators? "War gaming" - in other words team training involving a simulated cyber emergency - can be invaluable to expose any defects in current protocols and practise mobilising for a data breach or cyberattack.

Getting help

Norton Rose Fulbright LLP has a dedicated Information Governance, Privacy and Cybersecurity team. We can help you with getting up to date on protecting your scheme's systems and data, and we can also be there for you if a cybersecurity incident does occur. If you would like to know more, please get in touch with your usual Norton Rose Fulbright pensions contact.

Contacts

Lesley Browning
Partner
Tel +44 20 7444 2448 | +44 77 1030 3311
lesley.browning@nortonrosefulbright.com

Shane O'Reilly
Partner
Tel +44 20 7444 3895
shane.o'reilly@nortonrosefulbright.com

Steven Hadwin
Director, Head of operations - Data protection, privacy and cybersecurity
Tel +44 20 7444 2290
steven.hadwin@nortonrosefulbright.com

NORTON ROSE FULBRIGHT

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3700 lawyers and other legal staff based in Europe, the United States, Canada, Latin America, Asia, Australia, Africa and the Middle East.

Law around the world

nortonrosefulbright.com

Norton Rose Fulbright Verein, a Swiss verein, helps coordinate the activities of Norton Rose Fulbright members but does not itself provide legal services to clients. Norton Rose Fulbright has offices in more than 50 cities worldwide, including London, Houston, New York, Toronto, Mexico City, Hong Kong, Sydney and Johannesburg. For more information, see nortonrosefulbright.com/legal-notices. The purpose of this communication is to provide information as to developments in the law. It does not contain a full analysis of the law nor does it constitute an opinion of any Norton Rose Fulbright entity on the points of law discussed. You must take specific legal advice on any particular matter which concerns you. If you require any advice or further information, please speak to your usual contact at Norton Rose Fulbright.

35483_EMEA – 08/21