STEPHENSON HARWOOD

pensions law group

Cybersecurity: is your pension scheme prepared for the expected? Fail to prepare; prepare to fail.

Introduction to the increasing cyber threat

The level of cybercrime continues to grow at an unprecedented rate in the UK and across the globe, with UK Government figures from 2021 showing that nearly 40% of businesses surveyed had suffered cyber security breaches or attacks in the last year. Over recent years the threat of attacks has been exacerbated by the increase in staff working from home, and from increased political tensions and activity from hostile states.

Ransomware continues to be a focus of cybercriminals and is now the most prominent and immediate cyber threat to UK businesses, and one which should be at the top of the agenda for pension schemes. However, many schemes, trustees and administrators seem to be inadequately prepared, with a recent Aon report highlighting that only 2 in 5 schemes have a robust incident response plan, and that the majority of schemes believe that they can rely on their sponsor's cyber security resources in the event of an incident (which will neither be tailored to the scheme, nor likely tested as being an appropriate solution).

Key takeaways

- Trustees are ultimately responsible for managing cyber security as part of their effective governance and controls.
- The current threat level is high, and pension funds are a likely target.
- The scheme supply chain often creates the most material vulnerabilities.

Key actions

- Audit and test technical security measures in place.
- Review, refresh and test response plans.
- Map, audit and test supply chains.
- Produce a "grab sheet" with key information on a couple of pages.
- Engage third party professionals – forensic IT and legal – so they are available in an emergency.
- Refresh training to trustees and key stakeholders.

There seems to be no obvious trend in the target of ransomware attacks, other than being levied against organisations which have the means to pay the demands and would face immediate (financial, reputational, and regulatory) pressures to resume business as usual. This makes pension schemes, and those operating in their management and supply chain, extremely susceptible to attacks.

In this latest insight we look at why pension schemes are particularly exposed, the regulatory landscape and the accountability of trustees, and cover the technical and practical ways that schemes can prepare for, and plan their response to, an inevitable attack.

Pension Schemes as a key target

Pension schemes are at a heightened risk of being subject to attacks from cybercriminals due to several key factors:

- They hold a significant amount of valuable and sensitive data (including personal data and scheme data) – this can be sold by attackers on the black market or encrypted as part of a ransom request.
- It is imperative that schemes can maintain their payments to beneficiaries without interruption – this puts pressure on schemes to comply with ransomware attacks in order to operate as usual.

- It is relatively well known (from several industry surveys) that many schemes are under prepared – it is important to understand that cybercriminals are now "professionals", undertaking their own detailed research on who to attack and on which sectors are most vulnerable.

Pension schemes also typically have complex supply chains, with significant administration and specialist services being outsourced. This results in a number of weak points in the integration of services and systems and opens up vulnerabilities that cybercriminals can exploit. From an internal perspective (and for those schemes that run more functions in-house), internal IT functions may be under resource pressure, and systems may be outdated, which adds to the exposure risk.

What is at risk?

Cyber security breaches or attacks carry a number of risks to pension schemes, including:

- data loss – sensitive personal and financial data could be exposed to third parties;
- business interruption – systems could be corrupted, or encrypted beyond use;
- extortion – ransomware attackers request payments for de-encrypting data and systems;
- additional expense – breach remediation can be costly and a drain on internal resources;
- exposure to regulatory fines – the scheme could be fined for breach of its legal obligations;
- reputational damage – adverse publicity can be damaging to the scheme and the sponsoring employer; and
- legal claims - individual and group actions could be taken against the scheme.

Regulatory requirements

Unsurprisingly, the Pensions Regulator (**TPR**) views cyber security as a significant risk issue for pension schemes and in March 2021 set out new expectations for trustees in the draft single code of practice. This builds upon more high-level requirements under the Pensions Act 2004 that impose legal requirements to establish and operate an effective system of governance and internal controls.

By way of example (from a long list of requirements), the draft code of conduct includes the following expectations on scheme governing bodies to:

- have clearly defined roles and responsibilities to identify cyber risks and breaches, and to respond to cyber incidents;
- assess, at appropriate intervals, the vulnerability to a cyber incident of the scheme's key functions, systems and assets (including data assets) and the vulnerability of service providers involved in the running of the scheme;
- consider accessing specialist skills and expertise to understand and manage the risk;
- maintain a cyber incident response plan in order to safely and swiftly resume operations; and
- take action so that policies and controls remain effective.

The inclusion of cyber security in the new draft single code of practice represents a shift from the current position of cyber security being dealt with under TPR's guidance. Courts or tribunals **must** take into account the provisions of codes of practice (unlike with guidance) when determining if trustees have met their legal requirements. It is anticipated that the new draft single code of practice will be in force in Summer 2022. Governing bodies will need to carry out a review of their cyber security policies to ensure they meet the expectations set out in the code.

At a general level, trustees and scheme managers are required by law to establish and operate adequate internal controls to ensure their scheme is operated in accordance with scheme rules and regulatory requirements. A key part of this requirement is to have controls, processes, and policies to identify and manage risk (including those arising from a cyber security perspective).

Alongside the oversight of TPR, trustees must also comply with their obligations under UK data protection laws, including the obligations under the UK General Data Protection Regulation to

have clearly documented policies and implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. This is a broad obligation and imposes duties to ensure both internal and external systems are robustly protected.

In the event of a cyber-attack, the trustees (and potentially other connected data controllers affected by the breach) must report any personal data breach to the Information Commissioner's Office ("**ICO**"), unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals concerned, and in some instances they must also communicate the personal data breach to the data subjects themselves.

It is worth noting that an incident may be reportable even if data is not extracted or publicly released – unauthorised access to personal data constitutes a personal data breach under the UK GDPR and can trigger reporting obligations.

Penalties for non-compliance with data protection laws can be up to the greater of £17.5m or 4% of total annual worldwide turnover.

Trustee accountability

Trustees, as guardians of the scheme, are ultimately accountable for the security of scheme assets and information, irrespective of whether these are delegated or outsourced to third parties - trustees are ultimately responsible for ensuring that the pension scheme is run properly, and that members' benefits are secure. Therefore, protecting against cyber security risk is a fundamental element of compliance with a trustee's legal and fiduciary duties, and ultimate responsibility cannot be outsourced.

Ultimately, trustees are responsible for ensuring appropriate technical and organisational measures are implemented to keep data secure, and proactive and reactive plans are in place to govern and mitigate cyber security risks.

The main cyber security threats

Ransomware, a form of malware, is now the biggest cyber threat to most businesses, including pension schemes. This malicious software is used to encrypt target data and disable access to systems, so that cybercriminals can extort a ransom in exchange for the decryption key.

Typically, ransomware attacks are delivered through phishing emails, that then enable attackers to gain access to the underlying network to deploy encryption software on the data assets. In combination with this, cybercriminals also often extract files and data that they can share with the target as proof of their control and access over the network. They also often threaten to release these files and data if the ransom is not paid.

This type of attack would paralyse a pensions scheme, by disabling access to systems and data, preventing business as usual transactions with beneficiaries, and threatening the security of underlying sensitive financial data. As a result, schemes are in the difficult position of having to consider paying the ransom demands, often in cryptocurrencies that are almost impossible to recover at a later date.

When faced with the prospect of paying a ransom demand, careful consideration needs to be given to compliance with anti-money laundering regulations and international sanctions and counter-terrorism legislation. In most instances such payments aren’t illegal.

Other key threats include:

- Phishing: seeking to obtain information whilst appearing to be from a legitimate source or contact. These attacks can be used to target individuals (spearfishing) e.g., to appear to be a genuine email from a CFO requesting a revenue controller to make an urgent payment or to request sensitive payment details.

- Hacking: gaining access to systems via IT vulnerabilities to steal information, such as bank account details, or to obtain valuable intellectual property. There are also threats from hacking from individuals who hack systems as a "hobby", or to test and train their cyber skills.
- Data leakage: obtaining access to data through vulnerabilities and unauthorised transmissions – these can occur through the sharing of unencrypted files, or backdoors on websites. Data leaks by internal personnel, both by error and maliciously, also pose a threat.

Supply chain risks

When considering cyber vulnerabilities, it is imperative that the analysis covers all potential supply chain vulnerabilities. Whether that is scheme administrators, suppliers of internal systems, or other third-party service providers. These can often be easy and rewarding targets for cybercriminals, as gaining access to their environment may more easily allow access to multiple underlying end users.

In order to assess these potential risks, it is important to gather relevant information, undertaking a detailed mapping exercise to understand what third parties are being engaged, the nature of the services they provide, what access they have to underlying scheme data and financials, and what access and integrations there are into the scheme's systems (or systems of other suppliers). To kick off this mapping exercise, it can be helpful to work with finance and IT teams to run through each supplier engaged by the scheme.

This information can then be used to create a supply chain risk map, to categorise "high risk" suppliers and particular vulnerabilities.

The next step is to conduct a detailed review of the obligations and protections set out in each contract. For example, checking that the contracts impose adequate minimum-security requirements, rights to conduct penetration testing (where appropriate), and contain audit rights and security breach notification requirements. It is also important to consider the contractual allocation of risk and governance responsibilities, liability and exclusions, and gather information on reporting lines and key contacts.

In relation to new contracts (or renewals of existing contracts) now is a good time to ensure that procurement policies and standard templates - contracts, security requirements, governance schedules etc. - are appropriate and up to date.

In assessing and managing the supply chain risks, it is important to:

- document key contractual information, reporting obligations and contact details in an easily accessible format – in the event of a breach, it is vital to have this basic information readily to hand;
- ensure documented minimum-security requirements are kept under review to ensure they reflect industry best practice;
- maintain a dialogue with key suppliers to understand how they are taking action to mitigate evolving cyber risks;
- carry out security audits to ensure suppliers are complying with their security and data handling obligations,
- where relevant, carry out routine penetration testing on supplier systems and interfaces (or ensure suppliers carry out and report back on such testing); and
- include your key suppliers in your business continuity plans and get them to participate in continuity testing activities.

What should pension schemes be doing to implement appropriate security measures?

Pension schemes typically lack expert dedicated IT resources, and so third-party specialists should be engaged to assist with implementing, monitoring, and updating technical security measures.

As a minimum, pension schemes should ensure that the following security fundamentals are implemented:

- carry out regular (or ideally real-time) back-ups of systems and data and implement continuity arrangements for failover support;
- monitor the network to check for suspicious activity or unauthorised access - typically using endpoint threat detection and response (ETDR) software;
- disable the use of removeable media such as USB memory sticks or ensure that systems force scans on them for malware;
- limit access controls to highly sensitive data and systems to only those that need access to fulfil their specific role;
- regularly test networks and systems for vulnerabilities and test the interfaces and data exchanges with third parties;
- ensure staff are trained on cyber security, have read, and understood policies on the acceptable use of IT, and are aware of their own obligations to maintain security and confidentiality of scheme assets and to report any potential breaches; and
- monitor key threats and updates, such as from the National Cyber Security Centre who publish threat reports (and provide other excellent resources and services).

Cyber incident response planning

It is almost impossible to respond to, and mitigate the effect of, a cyber security breach or attack if you do not have adequate response processes and tools in place. However, the temptation is often to produce lengthy, detailed, policy documents and response plans. These can be useful reference points when checking security requirements or supplier assurance steps during a procurement process, but they aren't necessarily helpful on a Friday afternoon when an incident comes to light (and in practice, can be so cumbersome they are totally disregarded).

From our experience, to supplement any detailed policy document, pension schemes should ensure that they have a short "grab sheet" of no more than a couple of pages that documents the key information. This should set out contact details of who forms the initial response team - including details of external third-party specialists, such as forensic IT consultants and legal advisors – and a prioritised checklist of actions to initiate. This will ensure that the "first responders" can be mobilised quickly, and critical containment activities can be implemented without delay.

Bringing all of this together, set out below are our top tips for incident response planning:

- produce a grab sheet, keep it updated, and keep it to hand;
- set up notification email addresses – one for reporting potential incidents, and one to cascade internal notifications;
- build a good relationship with an IT consultancy business that can deploy forensic IT specialists on immediate notice to assist with initial investigations and containment activities;
- engage external legal counsel on a retainer – you need to know a trusted legal advisor who can step in and support on critical incidents (and you don't want client/matter onboarding admin to delay their ability to respond and advise);
- ensure you understand any legal reporting obligations to TPR and the to the ICO, including applicable timescales;
- raise awareness of cyber risks across the scheme by ensuring everyone has participated in relevant on-going training;
- ensure key stakeholders, and in particular those listed on the grab sheet, are trained on handling a cyber incident; and
- understand the terms of any insurance cover, including breach notification requirements (which should be noted on your grab sheet).

STEPHENSON HARWOOD

pensions law group

We are here to help

Cyber risks will continue to evolve at a rapid pace, and the risk levels in the UK are likely to remain high for the immediate future. Pension schemes therefore need to maintain their resilience to cyber-attacks, and ensure that their internal controls, governance, and planning are up-to-date and fit for purpose.

Should you wish to discuss any of the matters raised in this insight, or require assistance with reviewing and updating your organisational cyber security measures and response plans, please contact one of our experts and we will be happy to discuss further.

Our cyber security services

- Regulatory guidance
- TPR code compliance
- Supply chain audits and risk mapping workshops
- Policy reviews and updates
- Bespoke training sessions
- Response planning – grab sheets and containment plans
- Incident management and advice on regulatory notification

Contacts

Simon Bollans
Partner
Commercial, Outsourcing & Technology
T: +44 20 7809 2668
E: simon.bollans@shlegal.com

Naeem Noor
Senior Associate
Pensions
T: +44 20 7809 2092
E: naeem.noor@shlegal.com

STEPHENSON HARWOOD