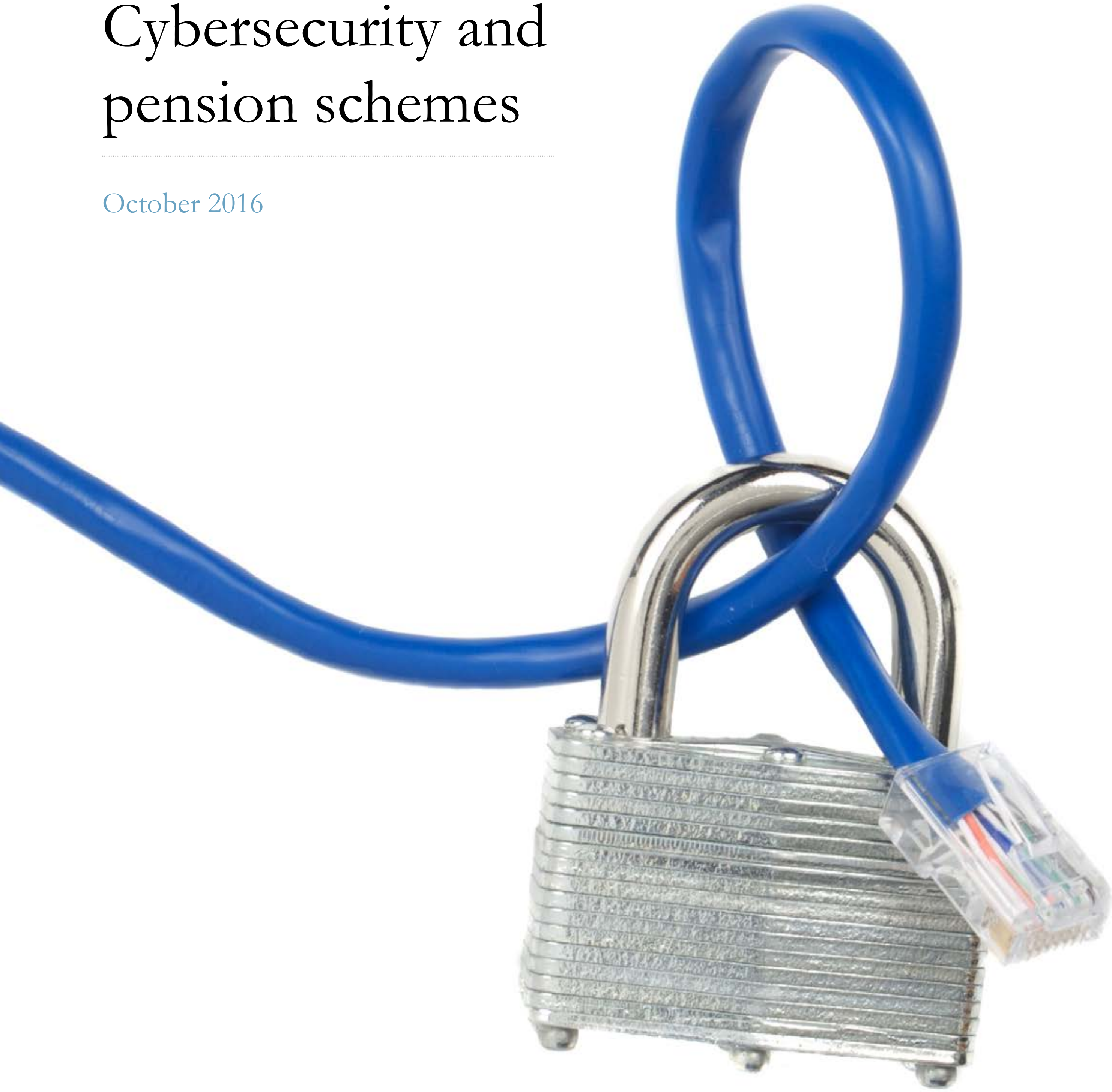
ALLEN & OVERY

Cybersecurity and pension schemes

October 2016



Cybersecurity and pension schemes

Cybersecurity has become a very hot topic for commercial organisations, with multiple major hacking attacks hitting the headlines in recent years. Pension schemes have not yet been the subject of a high-profile attack, but that doesn't mean they are immune. This is an area where trustees should be acting – and quickly – to ensure that members' interests, and their data, are protected.

What's the relevance for pension schemes?

Personal data has become an increasingly valuable commodity, and pension schemes hold an enormous amount of it. For any member, their pension scheme will hold records of their name, address, NI number, date of birth, salary information, and so on. For some members, it will also hold sensitive personal data about health issues and family members. For pensioners or members who have accessed DC funds flexibly direct from the scheme, it will hold bank details. A hacker might even be able to identify individual members, or beneficiaries of a deceased member, who have been paid significant lump sums. All this information is valuable, both to fraudsters who might want to access and steal it, and to 'hacktivists' who might want to destroy it.

Research[1] shows that trustees perceive the risk of fraud linked to their IT systems, member records or identity theft (at 7%, 5% and 8% respectively) as being much lower than the fraud risk attached to pension scams (59%) or even pensioner existence (18%). This clearly reflects areas that trustees have been asked to focus on in recent years, such as pension liberation and scam risk following the introduction of flexible access in April 2015. However, it also suggests that there is a general lack of awareness about the potential for schemes to be affected by cybersecurity breaches.

Legal drivers and legal risks

Data disruption could play havoc with pension scheme processes, from record-keeping to paying benefits, so there are solid practical reasons for taking action. However, there are also overriding legal drivers: as data controllers, trustees are required to take 'appropriate technical and organisational measures' to guard against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Cybersecurity is just one aspect of this.

In addition, trustees are required to operate internal control mechanisms which ensure that schemes are run in accordance with both their own rules and the law. That includes arrangements for the administration and management of the scheme, and for the safe custody and security of scheme assets. It's for trustees to identify the type of risks which affect the scheme, and the likely incidence and impact of potential risks occurring – but the Pensions Regulator has now said that all trustees should regard cybersecurity as a key risk, which should feature on their risk register. Trustees therefore need to consider what controls they should apply to mitigate cyber risks, including the legal risks triggered by a breach of cybersecurity.

Safeguarding information assets

When we talk about a duty to safeguard the scheme assets, we traditionally mean the financial assets and investments of the scheme. However, this could appropriately be given a wider meaning. A pension scheme cannot function without its membership data; gaps and discrepancies cost time and money to repair, so clearly the data has value to the scheme. It also has value to the members to whom it relates – for many members, their pension rights are likely to be their most significant financial asset, so a member's DC pot, for example, should be safeguarded as securely as cash in the bank. Finally, of course, the data has huge potential value to fraudsters who might want to steal it.

Understood in this way, cyber risks which threaten scheme data should be taken as seriously as other legal, regulatory, financial or operational risks to the assets of the scheme.

[1] RSM Pension Fraud Risk Report 2015

What do cyber risks look like?

Cyber risks take many forms, and need to be tackled from many angles. It’s not simply a matter of bolting on extra software. In the pension scheme context, cyber risks could include:

- Hacking attack against the scheme
- Loss of a laptop containing member data
- Human error by administrators with data access
- Hacking attack against third party administrator
- Virus or malware introduced to system
- Trustee falling victim to a phishing email

Cybercriminals will look for the weakest link in an organisation’s security in order to make their attack; it is trustees’ responsibility to do all they can to ensure that the pension scheme is not the ‘soft underbelly’ of the wider corporate group.

How bad could the damage be?

The damage caused by a breach in cybersecurity will depend on the type and scale of the breach and the data lost or stolen. It could, however, include any of the following:

- Service interruption
- Loss to members
- Loss or disclosure of member data
- Regulatory action and significant fines
- Ombudsman complaints or litigation
- Time and financial costs to the scheme
- Reputational damage externally
- Loss of member confidence
- Direct impact on pensioners if payments are disrupted
- Claims for compensation – financial loss or distress and inconvenience
- Downtime of scheme website
- Reporting obligations

What should trustees do?

1. Make a plan

Carry out a risk assessment of data security in all aspects of pension scheme business, both internal and external. Government-commissioned research[2] has found that 75% of large organisations have suffered staff-related security breaches, whether accidentally or otherwise; security starts at home.

Audit your cyber and data risks: who holds your data? What processes do they have in place? Our checklist of questions (see pages 8 and 9) will give you some starting points to consider, but your own approach will be scheme-specific. Arrange training for the trustee board and other relevant personnel on cybersecurity, data encryption, passwords, etc.

Design a plan to reduce the chance of a successful cyber-attack and to limit the consequences of any cybersecurity breach. This is likely to link to the approach developed by the scheme sponsor. It should include an incident management plan, with clearly delineated roles and reporting lines, from detection of a breach, through notification requirements, to remedying the weakness in security.

Ensure that your considerations and actions are recorded appropriately on your risk register.

2. Test the plan

Testing is the best way to identify any gaps in your security. Remember that even if budget constraints apply, there are simple measures you can take to mitigate any weaknesses you identify. These could include:

- providing training on data protection and security, including using online resources such as the government's CyberEssentials toolkit;
- reminding employees/trustees of the importance of using strong passwords and data encryption on detachable media;
- minimising transmission of personal data (for example, correspondence among members of the trustee body about an ill-health early retirement application); and
- ensuring that your contracts with third parties who hold your data require them to be vigilant.

Larger schemes may be able to go further, but all schemes should be able to take these relatively simple steps, and failure to do so is likely to be a breach of duty and/or maladministration. The Information Commissioner's position, for example, is that encryption is a basic measure: where data loss occurs and encryption software has not been used, regulatory action may follow.

[2] 2015 Information Security breaches survey, pwc

3. Follow the plan

Having a cybersecurity plan is fast becoming essential for pension schemes, but it can be a double-edged sword. If you fail to follow it, it will become the standard by which you are judged. It's therefore vital that everyone involved with the scheme and its data is fully aware of the plan and their part in maintaining data security.

Remember that in addition to the potentially significant penalties which can be imposed by the Information Commissioner's Office, the Pensions Regulator has the power to impose penalties if a cybersecurity breach exposes a failure of internal controls. In addition, it is entirely possible that members affected by the breach – or inconvenienced because of it, even if their data is not affected – could claim for compensation on the basis of trustee maladministration.

4. Refresh the plan

As cybersecurity measures – and methods of attack – evolve, your plan will need to be reviewed and updated.

Jargon buster:

Cybersecurity: the range of measures used to prevent unauthorised access to computer systems.

Encryption: a basic measure which can prevent data being accessed or processed without authority. Data can be encrypted while it is stored (for example on a laptop or memory stick, or in a database), or while it is in transit (for example by email or a wifi network). However, data will remain vulnerable while it is decrypted for processing. Encrypted data remains vulnerable to attack such as infection with malware.

Malware: also known as a computer virus, a worm or spyware, this is software which is written and distributed with the specific aim of attacking a host computer system (for example, by spreading a virus, corrupting or stealing data, or crashing the system). It may be introduced to a system by individuals inadvertently clicking on malicious email attachments or website links.

Phishing: fraudsters may use a fake email or other forms of contact to trick individuals into revealing personal information (for example, login passwords, account numbers, etc). Sometimes a single user or department within an organisation is targeted (known as 'spear phishing').

Hacktivist: a hacker exploits vulnerabilities in internet-connected computer systems as a challenge, but a hactivist may wish to attack an organisation for political or ideological motives. The pension scheme could be attacked as an access point to the corporate group or individuals within the organisation.

Assessing data risk: a checklist of initial questions

Internal processes

– Do the trustees, and any internal pensions managers, handle data securely? Studies show that employees (or other internal parties) are major contributors to cybersecurity risk, whether due to inadvertent errors or deliberate action. Is further training required?

– Do your working practices need to be reviewed? For example, if member data is included in trustee board papers, are all trustee email addresses appropriately secure? It is not uncommon for pensioner trustees, in particular, to use a home email address rather than one which is within the organisation's information security perimeter. This could be your point of greatest vulnerability to malware or a phishing attack.

– Do you have documented policies covering data security, encryption, etc?

– Do you scan all removable media (memory sticks etc) for malware before allowing data to be imported onto your systems?

– Are your IT systems and processes up to date? How is data stored? Is it backed up securely?

– Does your liability insurance cover cybersecurity-related acts or omissions by trustees or their delegates? Do you need a specific policy to cover cyber risk?

Member access

– If you provide members with online access to their personal accounts, are appropriate security measures in place (for example, minimum password requirements and other identity checks)?

– Are members clear about how they can verify that communications from the trustees are genuine? Cyber-attacks often work by mimicry ('spoofing') – if an email looks genuine enough, the recipient may click on a malicious link within it, introducing malware into the system.

– Do members take data security seriously in relation to their pension savings? Members should be encouraged to take the security of their pension information as seriously as that of their bank account – for example, using strong passwords and keeping these separate from login details.

Service providers

- Ask your administrators about their cybersecurity plan. Does it adhere to a recognised industry standard (such as ISO27001)? Is it independently audited? What is their incident management plan in the event of an attack?
- Does your contract with your administrators include a clear allocation of cybersecurity risks and governance responsibilities, from minimum requirements, monitoring and reporting, to liability and compensation, in the event that a breach occurs?
- In the case of a bundled or wholly insured arrangement, is the provider able to give you assurances that controls are in place in relation to the issues listed above?

Contacts

Pensions

Maria Stimpson
Partner
Tel +44 20 3088 3665
maria.stimpson@allenovery.com

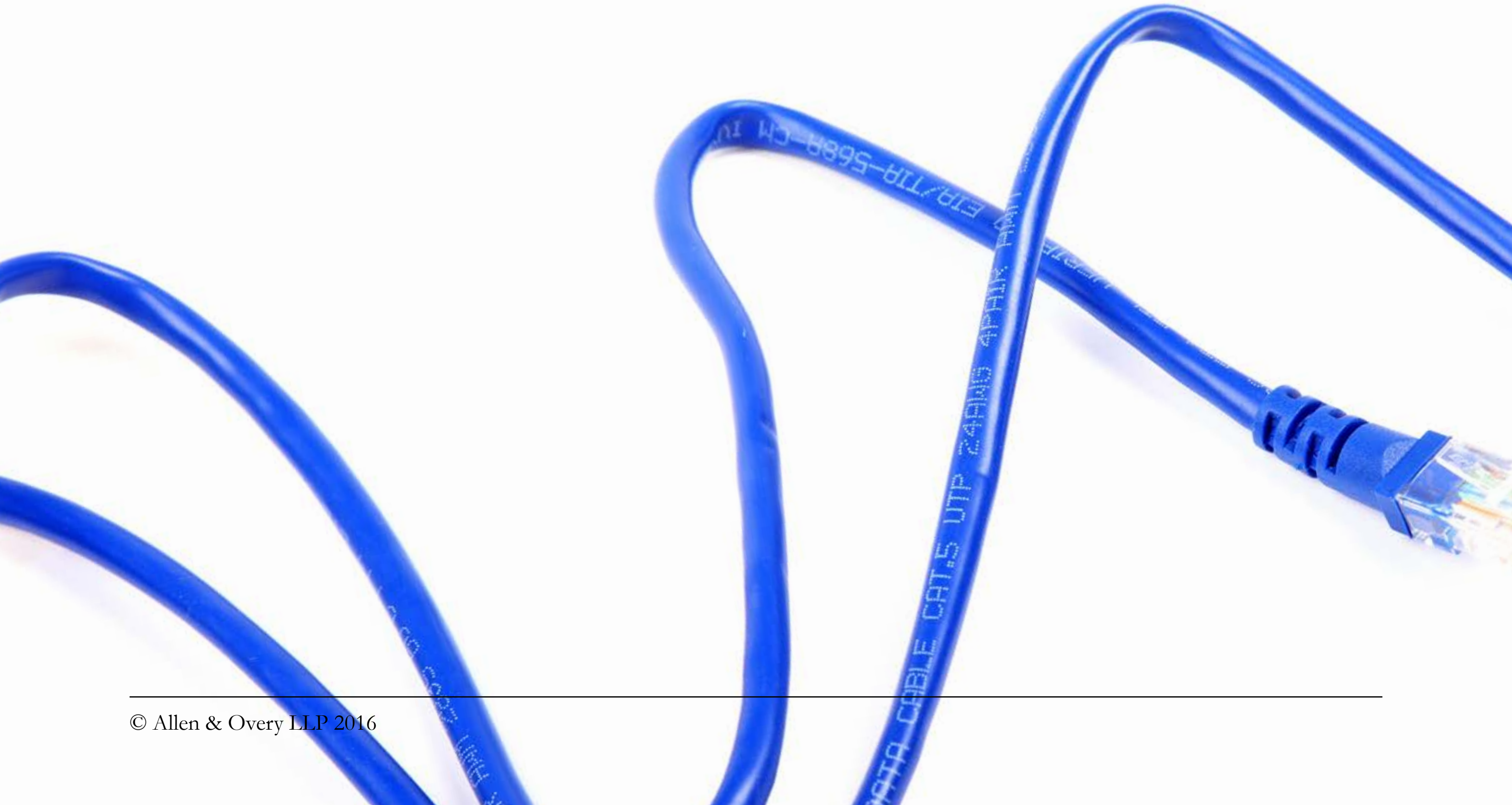
Däna Burstow
Partner
Tel +44 20 3088 3644
dana.burstow@allenovery.com

Neil Bowden
Partner
Tel +44 20 3088 3431
neil.bowden@allenovery.com

Jane Higgins
Partner
Tel +44 20 3088 3161
jane.higgins@allenovery.com

Andy Cork
Senior Associate
Tel +44 20 3088 4623
andy.cork@allenovery.com

Jason Shaw
Senior Associate
Tel +44 20 3088 2241
jason.shaw@allenovery.com



Cybersecurity

Lawson Caisley
Partner
Tel +44 20 3088 2787
lawson.caisley@allenovery.com

Jane Finlayson-Brown
Partner
Tel +44 20 3088 3384
jane.finlayson-brown@allenovery.com

Mark Ridgway
Partner
Tel +44 20 3088 3720
mark.ridgway@allenovery.com

Nigel Parker
Partner
Tel +44 20 3088 3136
nigel.parker@allenovery.com

How we can help

Clients turn to us to manage legal risk in relation to the threat of cyber-attacks. Allen & Overy's cross-practice team of cyber-incident response specialists supports clients to ensure they are resilient to cyber-attacks or other data breaches which may impact them. We act as a partner to make sure you can react quickly and effectively.

FOR MORE INFORMATION, PLEASE CONTACT:

London

Allen & Overy LLP
One Bishops Square
London
E1 6AD
United Kingdom

Tel +44 20 3088 0000
Fax +44 20 3088 0088

GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,200 people, including some 530 partners, working in 44 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

Abu Dhabi
Amsterdam
Antwerp
Bangkok
Barcelona
Beijing
Belfast
Bratislava
Brussels
Bucharest (associated office)
Budapest
Casablanca
Doha
Dubai
Düsseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Istanbul
Jakarta (associated office)
Johannesburg
London
Luxembourg
Madrid
Milan
Moscow
Munich
New York
Paris
Perth
Prague
Riyadh (cooperation office)
Rome
São Paulo
Seoul
Shanghai
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.
Yangon

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term **partner** is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings.

This document is for guidance only and does not constitute definitive advice.

allenovery.com