



PLSA NORTH LONDON GROUP: PENSION SCHEME FRAUD AND CYBER RISKS

Elisabeth Storey, Audit Director, RSM

27 November 2018

Pensions fraud and cyber security – a growing threat?



It's in the National Press...

Savers lose millions to retirement fraudsters

Andrew Ellson,
Consumer Affairs Correspondent



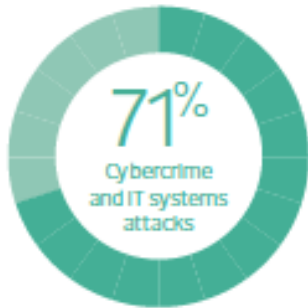
Surge in cybercriminals targeting pension pots

Savers are being tricked out of half a million pounds every day after a surge in criminals targeting British pension riches, *The Times* can reveal.

People with nest eggs to invest, including those with new freedoms to access their pensions, are falling for well-resourced foreign fraudsters impersonating the identities of legitimate companies.

Pension Scheme Fraud: our research

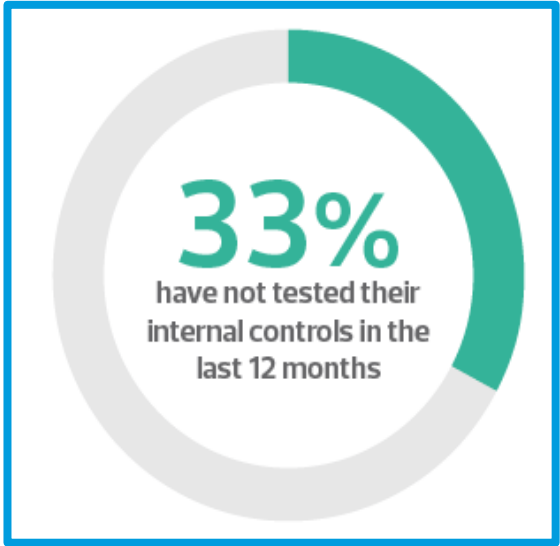
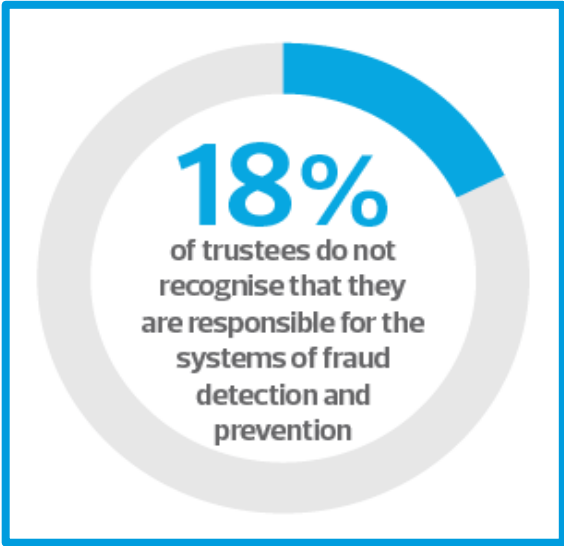
Perceived areas of vulnerability



Pension Scheme Fraud: our research



Pension Scheme Fraud: our research

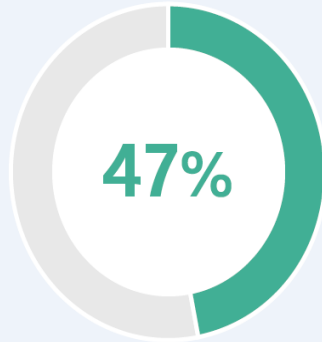


Pension Scheme Fraud: our research



Pension Scheme Fraud: our research

IT systems and cyber crime are the area of most vulnerability but only **47%** of respondents have received training in the last year



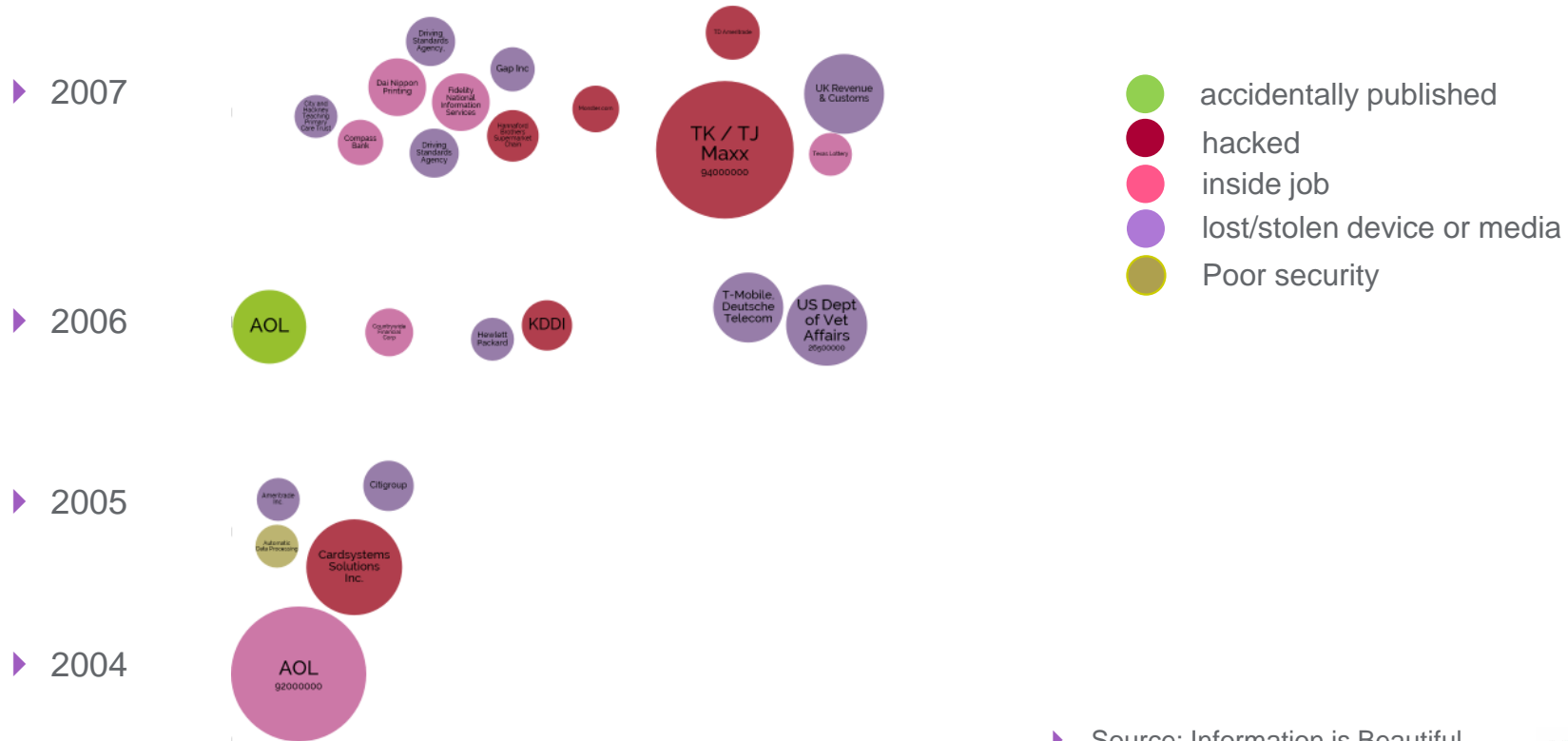
20%
have a 24-hour
incident response
plan to react to a
breach

A graphic featuring a blue arc at the top right, with the text '20%' in large blue font, and the following text in smaller black font: 'have a 24-hour incident response plan to react to a breach'.

Cyber - why is the position changing?

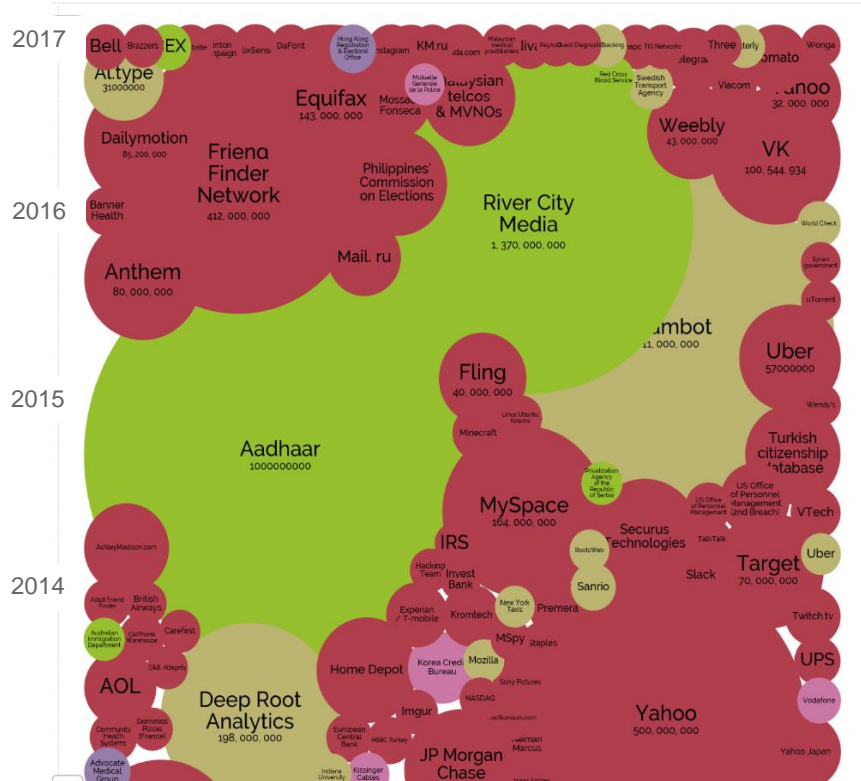


World's biggest data breaches – 10 years ago



▶ Source: Information is Beautiful

World's biggest data breaches – now



- accidentally published
- hacked
- inside job
- lost/stolen device or media
- Poor security

► Source: Information is Beautiful

Why the increase in risk?

Big Data & Analytics



Mobile Working



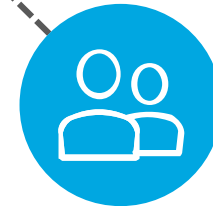
Internet of Things

Increase in ...

- ✓ Connectivity
- ✓ Access points
- ✓ Remote access
- ✓ Personal information
- ✓ Data sharing



Internet Transactions



Social Media

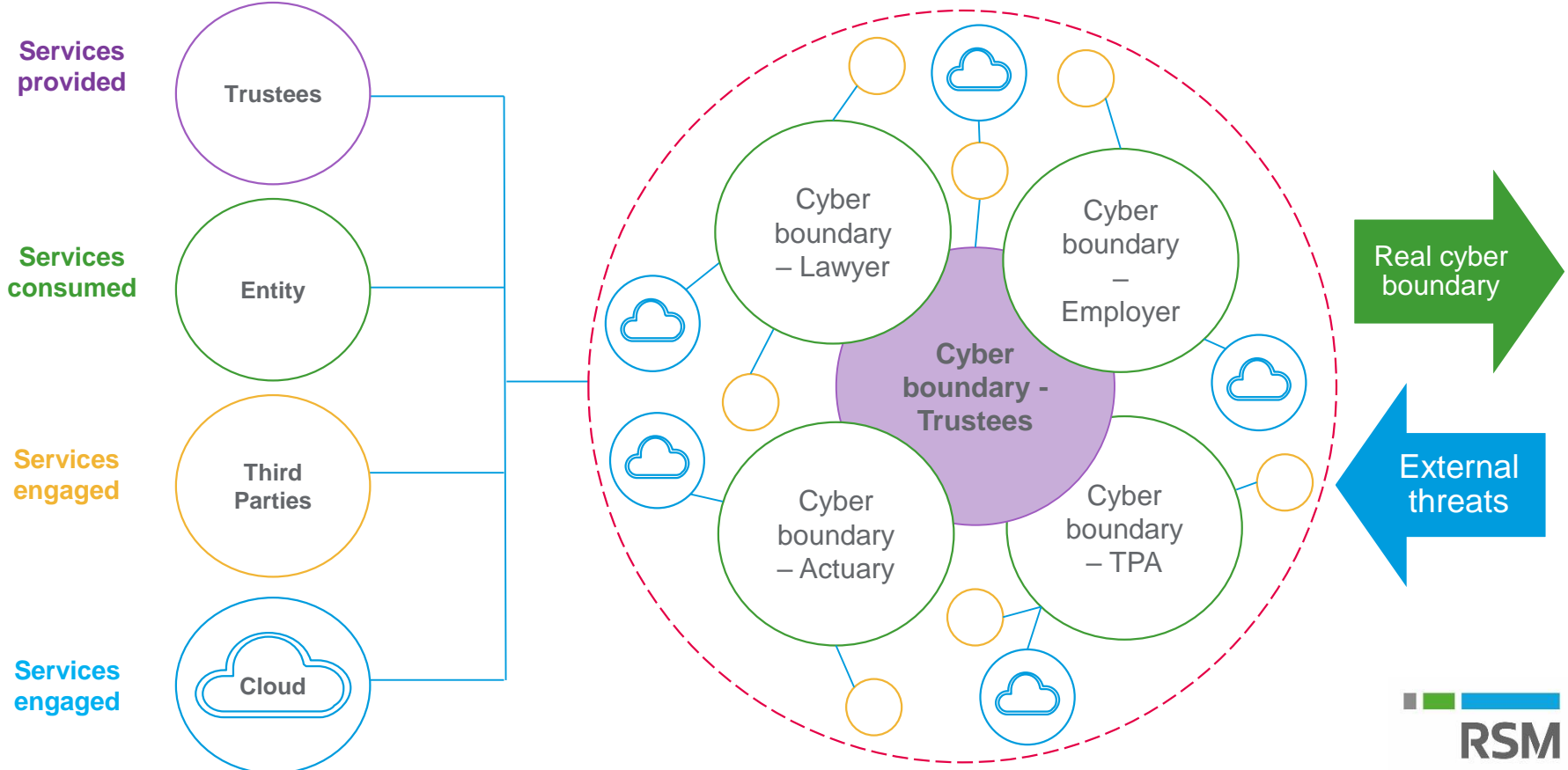
Wearable Technology



The Cloud



Understand your scheme's cyber footprint



Types of attacks



Insider
attacks



Phishing and
whaling

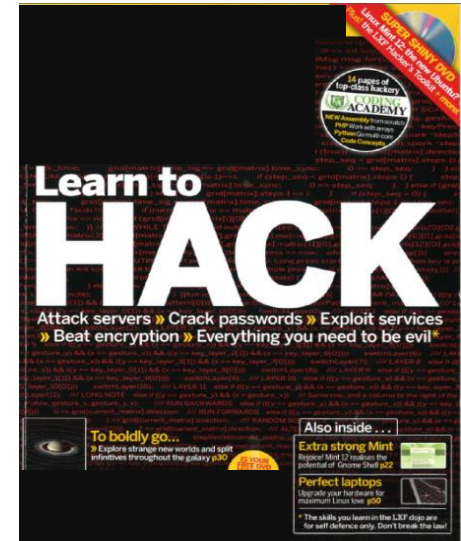


Vulnerability
attacks

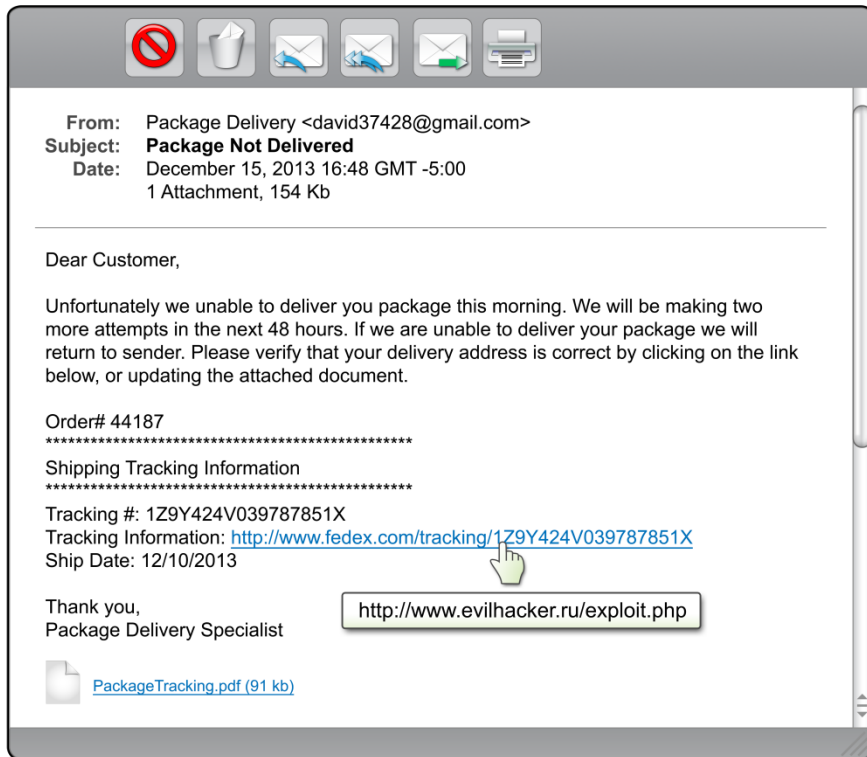


Ransomware

How easy is it?



Malicious content - ransomware



YOUR COMPUTER HAS BEEN BLOCKED

THE COMMON LAW IS THE WILL OF *Manibus* ISSUING FROM THE *Gr* OF THE *Propter*

THE UNITED STATES
DEPARTMENT OF JUSTICE

Your IP-address: 192.168.1.100
Your Provider: Microsoft Corp
Location: United States, Arizona

The work of your computer has been suspended on the grounds of the violation of the law of the United States of America.

Possible violations are described below:

Article - 184. Pornography involving children (under 18 years)
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic files)

Article - 171. Copyright
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files)

Article - 113. The use of unlicensed software
Imprisonment for the term of up to 2 years
(The use of unlicensed software)

ALL ILLEGAL ACTIVITIES CONDUCTED THROUGH YOUR COMPUTER HAVE BEEN RECORDED IN THE POLICE DATABASE, INCLUDING PHOTOS AND VIDEOS FROM YOUR CAMERA FOR FURTHER IDENTIFICATION. YOU HAVE BEEN REGISTERED BY VIEWING PORNOGRAPHY INVOLVING MINORS.

Video-recording: ON

In connection with the decision of the Government as of October 11, 2012, all of the violations described above could be considered as criminal. If the fine has not been paid, you will become the subject of criminal prosecution. The fine is applicable only in the case of a primary violation. In the case of second violation you will appear before the Supreme Court of the USA.

Amount of the fine is \$300. Payment must be made within 48 hours after the computer blocking. If the fine has not been paid, you will become the subject of criminal prosecution without the right to pay the fine. The Department for the Fight Against Cyberactivity will confiscate your computer (after 48 hours)

AN ATTEMPT TO UNLOCK THE COMPUTER BY YOURSELF WILL LEAD TO THE FULL FORMATTING OF THE OPERATING SYSTEM. ALL THE FILES, VIDEOS, PHOTOS, DOCUMENTS ON YOUR COMPUTER WILL BE DELETED.

The first violation may not entail the criminal liability if the payment of the fine in connection with the law of loyalty to the people, on 5 December 2012. In repeated violations of criminal responsibility is inevitable.

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of \$300.

How do I unlock computer using the MoneyPak?

1. Find a retail location near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash. A service fee of up to \$4.95 will apply.
3. To pay fine, you should enter the digits MoneyPak resulting code in the payment form and press Pay MoneyPak.

Green Dot MoneyPak

Code:
Status: Waiting for Payment 47:47:17

Where can I buy MoneyPak

Walmart RITE AID CVS/pharmacy
Walgreens Kmart

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires. In this case a criminal case against you will be initiated automatically.

AFTER PAYING THE FINE YOUR COMPUTER WILL BE UNLOCKED. (IN THE CASE OF SECOND VIOLATION YOU WILL BECOME THE SUBJECT OF CRIMINAL PROSECUTION WITHOUT THE RIGHT TO PAY THE FINE)

HOW ONE GANG SWIPED \$1BN FROM GLOBAL BANKS

Up to US\$1billion - £650million - has been stolen in approximately two years from financial institutions worldwide.

The fraud was detected by cyber security firm Kaspersky Lab in February 2015.

Gained entry into an employee's computer through 'spear phishing' – infected it with malware called Carbanak.



Sent authentic-looking emails from his account that other staff clicked on, spreading the malware through the bank.



Found the administrator account for the CCTV equipment

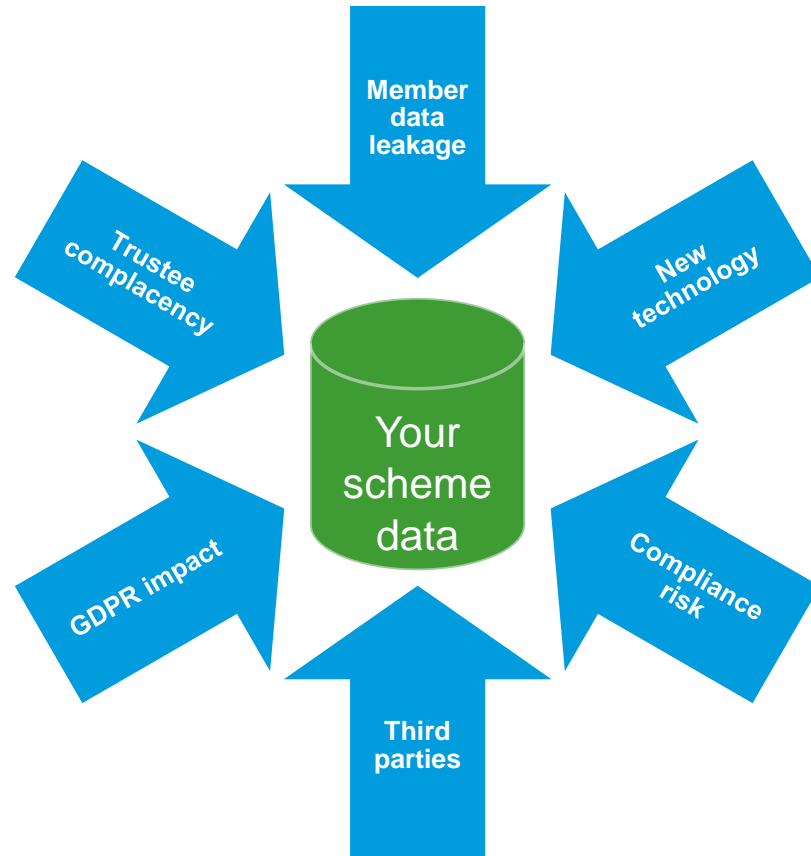


They used the CCTV to record everything that happened on the screens of staff who serviced the cash transfer systems.



They mimicked the activity of these staff activity in order to transfer money out.

Your data risks



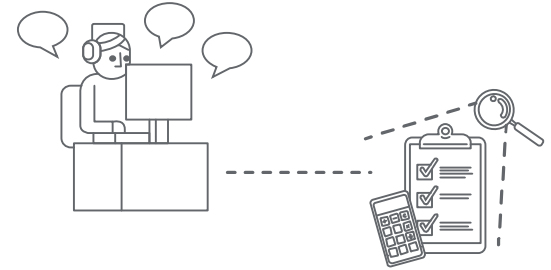
The challenges – the risks for pension schemes

Potential risks

- Lack of recognition/knowledge of data held
- Staff
- Complacency
- Poor internal processes
- Lack of investment and training
- Falling behind the curve

Potential results

- Loss of reputation
- GDPR brings significant fines for loss of data
- Loss of confidential information
- Loss of operational systems
- Loss of members' money – pots or pensions



What should Trustees be doing?



Questions to know the answer to



Where is my data?



Where does it go?



Who has access to it?



How is it used?

What about GDPR?



Further information

For more information visit www.rsmuk.com

To download the latest RSM fraud report, visit:

www.rsmuk.com/ideas-and-insights/pensions-fraud-in-2018

Questions

AUDIT | TAX | CONSULTING

Thank you

AUDIT | TAX | CONSULTING

The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM Corporate Finance LLP, RSM Restructuring Advisory LLP, RSM Risk Assurance Services LLP, RSM Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP, RSM Employer Services Limited, RSM Northern Ireland (UK) Limited and RSM UK Tax and Accounting Limited are not authorised under the Financial Services and Markets Act 2000 but we are able in certain circumstances to offer a limited range of investment services because we are members of the Institute of Chartered Accountants in England and Wales. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide. RSM Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317, to undertake reserved and non-reserved legal activities. It is not authorised under the Financial Services and Markets Act 2000 but is able in certain circumstances to offer a limited range of investment services because it is authorised and regulated by the Solicitors Regulation Authority and may provide investment services if they are an incidental part of the professional services that it has been engaged to provide. Baker Tilly Creditor Services LLP is authorised and regulated by the Financial Conduct Authority for credit-related regulated activities. RSM & Co (UK) Limited is authorised and regulated by the Financial Conduct Authority to conduct a range of investment business activities. Before accepting an engagement, contact with the existing accountant will be made to request information on any matters of which, in the existing accountant's opinion, the firm needs to be aware before deciding whether to accept the engagement.

© 2018 RSM UK Group LLP, all rights reserved

