PENSIONS AND LIFETIME SAVINGS ASSOCIATION

# PLSA SCOTLAND GROUP MEETING CYBER SECURITY

16 November 2023

Hymans Robertson, Edinburgh, Scotland

@ThePLSA

# AGENDA

15:00 **Registration** (light refreshments will be served)

15:25 **Welcome and Introduction**
**Heather Meighan,** (Chair, Scotland Group), Zedra

15:30 **Managing Cyber Risk for Pensions Schemes**
**Marion De Voy,** Principal, Mercer

15:45 **Q&A session**

15:50 **Pension Schemes and Cyber Security: Practical Issues for Trustees**
**Dan Boynton**, Senior Associate, Shepherd & Wedderburn

16:05 **Q&A Session**

16:10 **Coffee Break (5 mins)**

16:15 **Cyber Security: Data and Compliance**
**Lucy Stone,** Business Lead – Regulatory Policy, Analysis and Advice, The Pensions Regulator

16:30 **Q&A Session**

16:35 **Human Layer Security**
Our people are our biggest asset - and potentially our weakest link. How do we manage that?
**Brian Taylor**, Head of Information Governance and Group DPO, Hymans Robertson

16:50 **Q&A Session**

16:55 **Speaker Panel: Marion De Voy, Dan Boynton, Lucy Stone, Brian Taylor**

17:25 **Session Summary followed by Drinks Reception**

18:00 **Close**

# Managing Cyber Risk for Pension Schemes

**MARION DE VOY**

Mercer

Mercer

welcome to brighter

# Managing cyber risk for pension schemes

PLSA

16 November 2023

Marion de Voy, Principal, Edinburgh

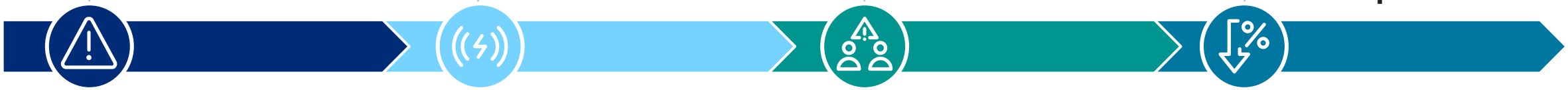
# Agenda

1. What is cyber risk?
2. Why is cyber risk important for pension schemes?
3. The Pensions Regulator cyber security requirements

# What is cyber risk?

# What is cyber risk?

## Cyber events can be malicious or accidental and result in a wide range of different impacts and consequences



### Cyber event

- Can be:
  - Malicious
  - Accidental
- Affects:
  - Data
  - Technology
  - Processes

### Leading to immediate impacts…

- Encrypted data
- Privacy violations
- Loss of access
- Phishing / fraud
- Bricked computers

### …requiring a response…

- IT forensics
- Legal advice
- Public Relations
- Crisis managers
- External bodies and authorities
- Regulators

### … and resulting in short and long term consequences

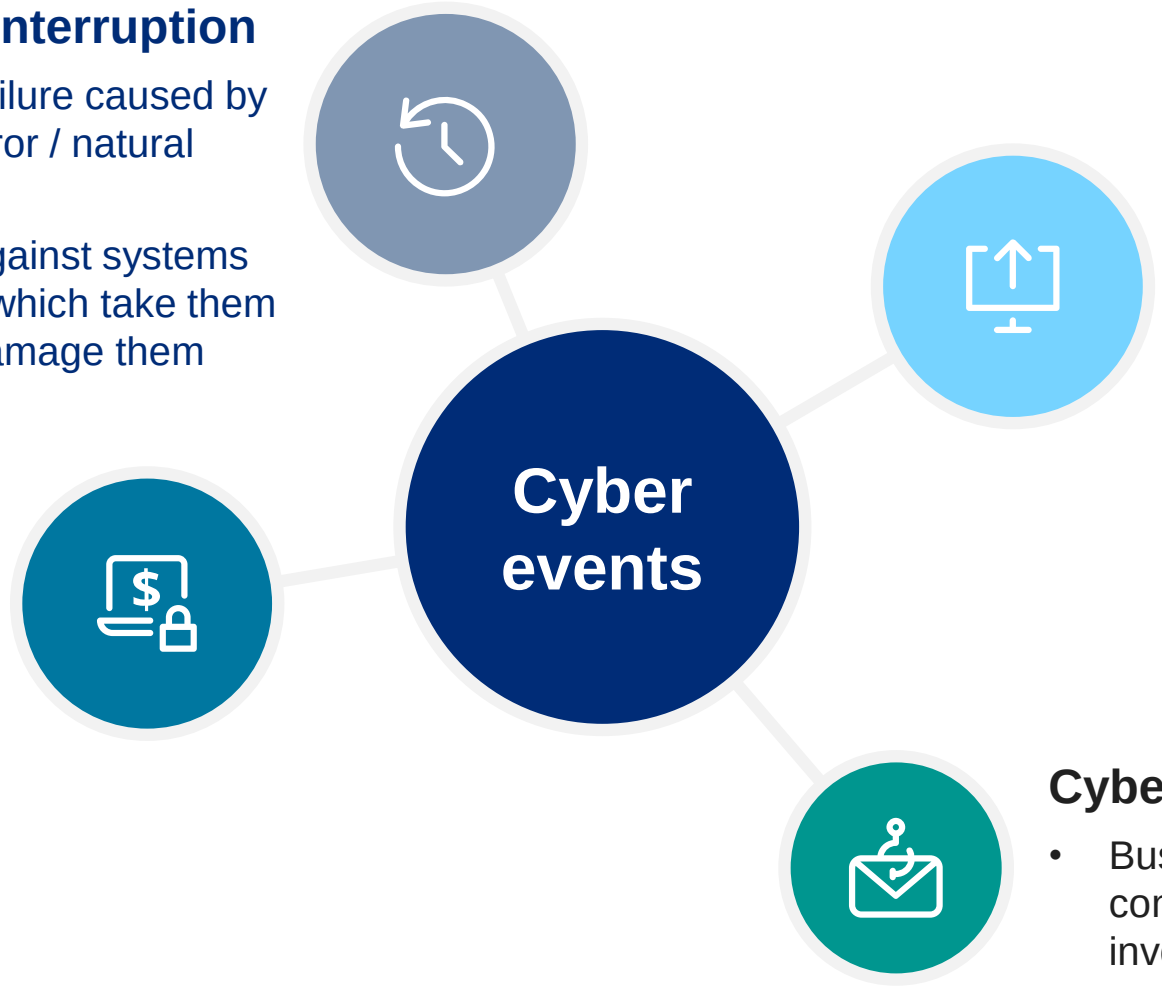
- 1st party costs
- Loss of income
- 3rd party liabilities
- Fines and penalties
- Litigation
- Reputation and brand damage

# How do cyber risks play out?

## Typically we see cyber risks take the form of one the following scenarios, however this list is not exhaustive

### Business interruption

- System failure caused by human error / natural causes
- Attacks against systems and data which take them offline / damage them




### Data breach

- Data sent to unauthorised person in error
- Cyber attackers steal personal data
- Internal employee maliciously discloses personal data

### Ransomware

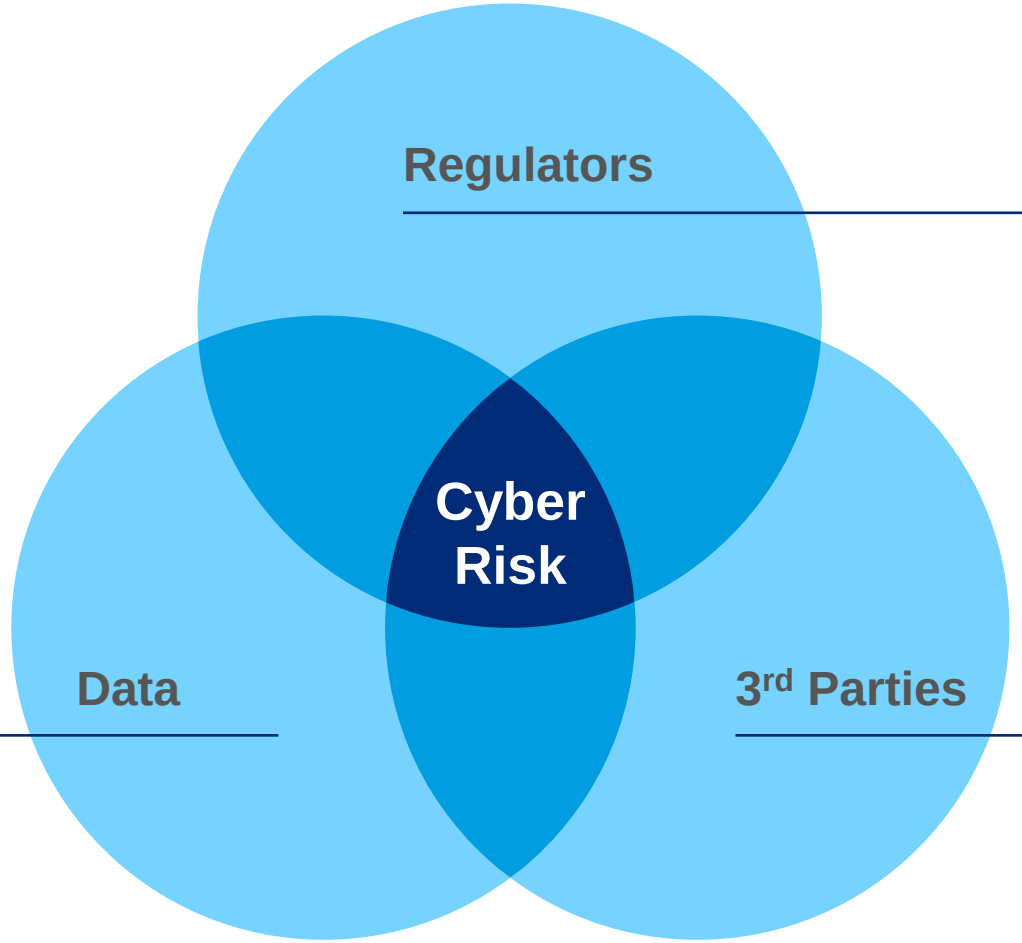
- Systems encrypted and users locked out and data stolen
- Extortion demands to restore systems and not disclose data

### Cyber enabled fraud

- Business email compromise / fake invoices leading to a payment diversion

# Why is cyber risk important for pension schemes?

# There are 3 main factors driving the increasing importance of cyber risk for pension schemes

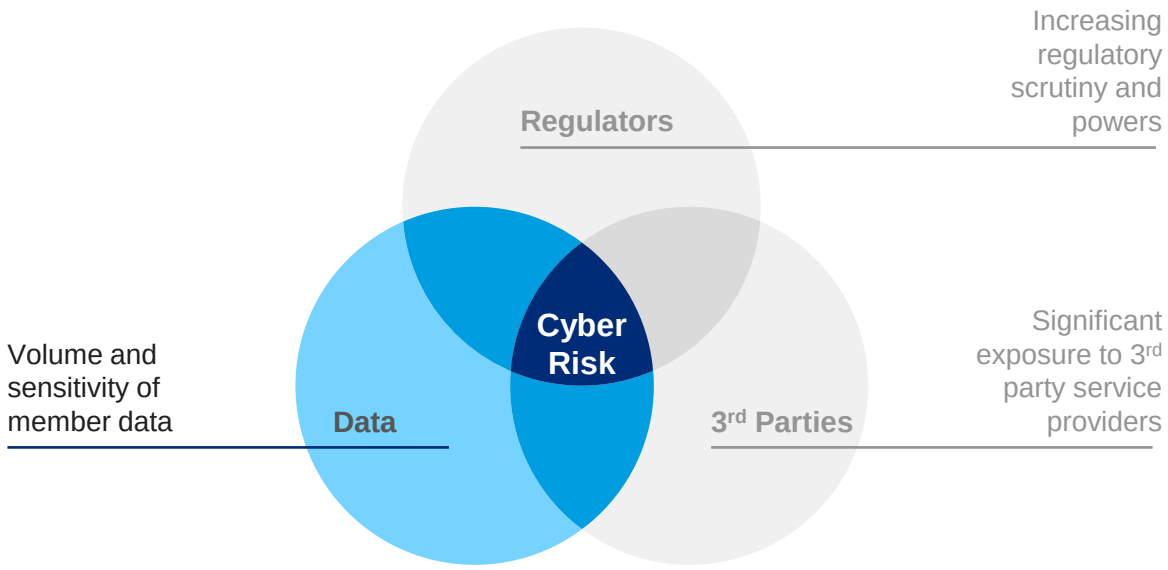



Increasing regulatory scrutiny and powers

Volume and sensitivity of member data

Significant exposure to 3rd party service providers

# Data exposure




*Pension schemes deal with large volumes of sensitive data records, including personal and financial information relating to members and employees.*

*This makes pension schemes and their eco-system of suppliers highly tempting targets for cyber criminals and other threat actors looking to obtain personal information through a data breach.*

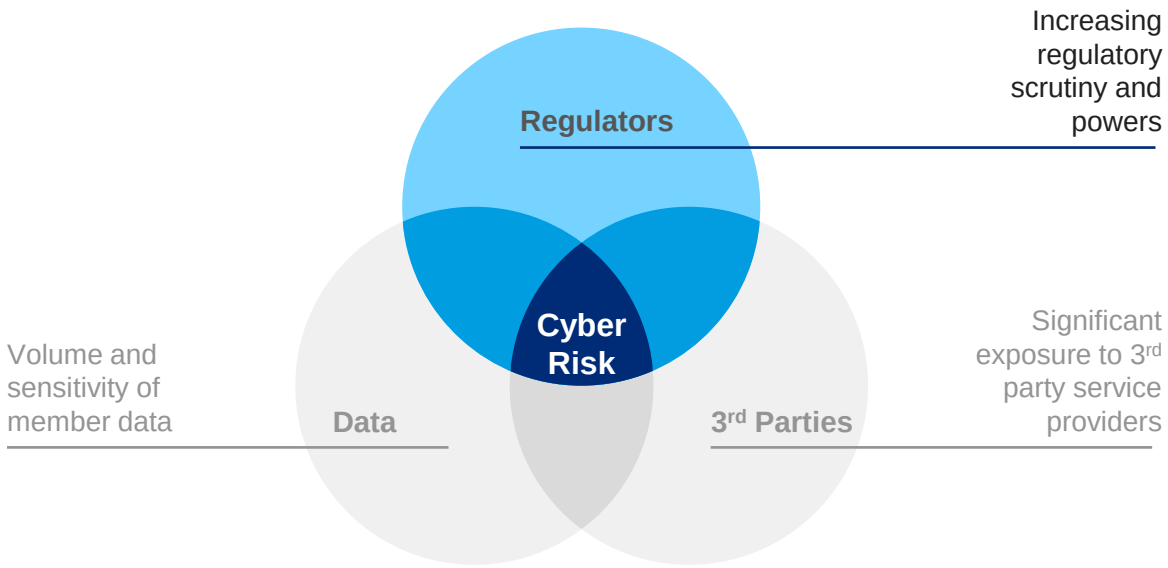
Key issues for trustees and scheme managers:

- Understand the **volume and sensitivity** of your data records
- Have a clear and documented view of **who data is shared with** and **how transfers are kept secure**
- Ensure controls are in place to **adequately protect the storage** of data records (including 3rd parties)
- Have a clear, documented plan in place to **deal with a data breach**

# Regulatory interest

Key issues for trustees and scheme managers:

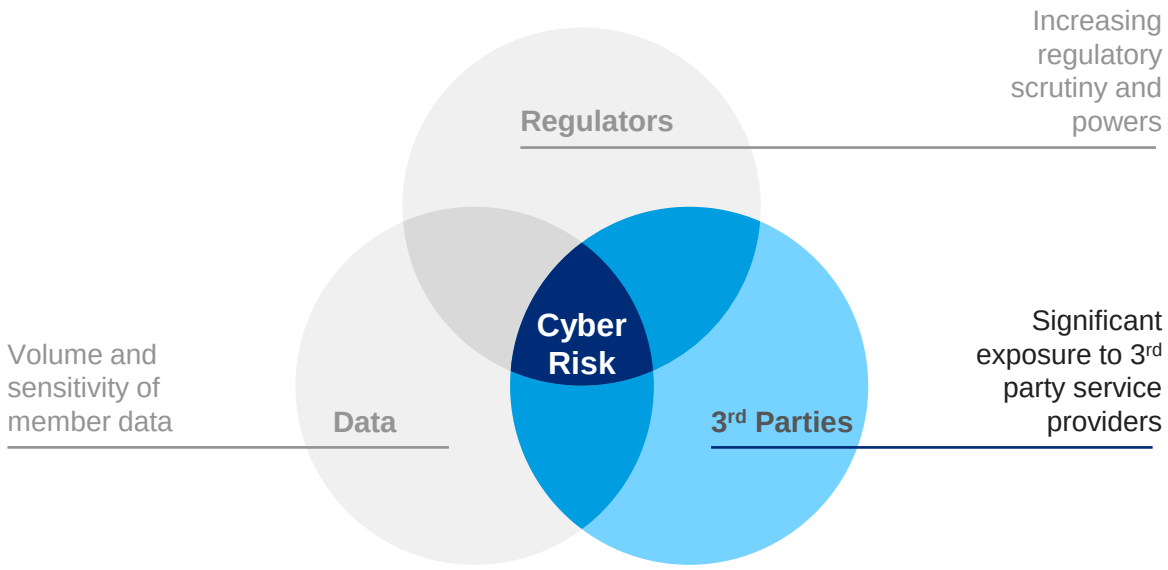
- Understand your obligations according to the guidance published by **the Pensions Regulator for cyber security**
- **Assess your cyber security measures against the regulatory guidance** and identify any areas where improvements are needed
- **Assess and incorporate** cyber risk for your scheme into your general approach to **risk management and governance**




*Sector specific regulators, including the Pensions Regulator, are increasing their scrutiny of the organisations under their purview for cyber security matters.*

*The Pensions Regulator has published specific guidance for pension schemes to follow in how they address cyber security. With the introduction of the GDPR / DPA 2018, there are also increased penalties for data breaches.*

# 3rd party exposure




*Pension schemes often outsource a significant portion of their activities to 3rd party suppliers, reducing the visibility and control over data and processes.*

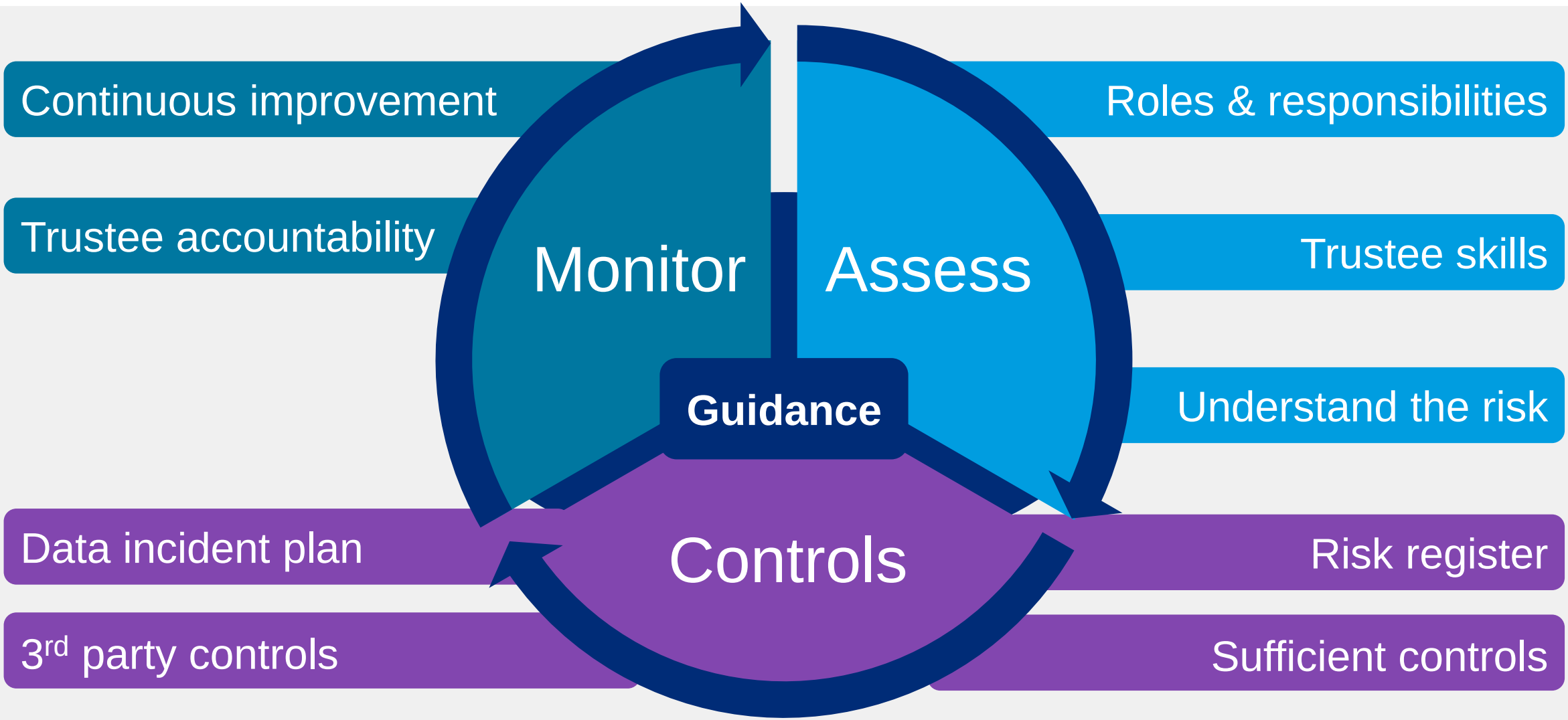
*Leveraging 3rd parties doesn't relieve trustees and scheme managers of their obligations for cyber security. Ultimately they are still accountable for cyber security and need to ensure 3rd parties are doing the right thing.*

Key issues for trustees and scheme managers:

- **Incorporate** cyber security and data protection requirements into contracts with 3rd parties and ensure they are **regularly reviewed**
- Seek **formal assurance** from your 3rd party suppliers as to the **robustness** of their cyber security capabilities
- **Review your suppliers' cyber security** as part of a regular, scheduled assessment (e.g. annually or once every 3 years)

# The Pensions Regulator cyber security requirements

# The Pensions Regulator: The basic principles



# What good looks like

## Assess and understand the risk

1. ***Trustees and scheme managers are ultimately accountable for cyber security***
   Being able to demonstrate to external parties that cyber security has been subject to the scrutiny of trustees and that appropriate action has been taken if needed.

2. ***You should ensure sufficient understanding of your scheme's cyber risk***
   Relevant cyber risks for the scheme should be identified along with the key technology and data assets that may be at risk.

3. ***You should have access to the required skills and expertise***
   Trustees should engage with external expertise (either through 3rd parties or the corporate sponsor) to ensure that cyber risks are adequately covered.

4. ***Roles and responsibilities should be clearly defined***
   Trustees roles and responsibilities should be formally defined and documented either as part of a stand alone security policy or incorporated into existing documentation.

# What good looks like

## Put controls in place

5 ***Ensure sufficient controls are in place***
Having understood the cyber risk which the scheme faces, controls should be put in place which limit the likelihood and impact of the relevant cyber risks.

6 ***Assure yourselves that all third party suppliers have put sufficient controls in place***
Contractual requirements should be in place for cyber security and 3rd parties assessed for the effectiveness of their cyber security measures.

7 ***Ensure an incident response plan is in place***
An incident response plan should outline key roles and responsibilities for decision making and a simple process flow for what to do in the event of a cyber risk occurring.

8 ***Be clear on how and when incidents would be reported to you and others, including regulators***
Should be part of a formalised incident response plan, with an outline of the process for communicating with 3rd parties and regulators.

# What good looks like

## Monitor and report

9

***Ensure cyber risk is on your risk register and regularly reviewed***
Cyber should be included as a discrete risk with an outline of the key cyber risks which have been identified and the associated controls.

10

***Continuous review and improvement***
Trustees should periodically revisit cyber security as part of their risk management process (e.g. once a year) and assess their current arrangements vs the past position.

# The Pensions Regulator: The basic principles

- Trustees & scheme managers are **ultimately accountable** for cyber security.
- Roles and **responsibilities** should be **clearly defined**.
- Trustees should have access to the required **skills & expertise**.
- Trustees should ensure **sufficient understanding** of your scheme's cyber risk.
- The cyber risk should be on your risk register and **regularly reviewed**.
- Trustees should ensure **sufficient controls** are in place.
- Trustees should assure themselves that all **third party** suppliers have sufficient controls in place.
- There should be an **incident response plan** in place.
- All individual trustees should be clear on how & when **incidents** would be **reported** to the Trustee and others, including regulators.
- Cybersecurity measure should be kept under a programme of **continuous review and improvement**.

# Summary

## Actions/next steps

Trustees should consider the following next steps as key priority actions to improve their cyber risk profile:

1. **Assess the scheme's cyber risk profile** to identify dependencies on technology, data and 3rd parties and the potential impact to the scheme if compromised by a cyber attack.
2. **Implement cyber security policy and a set of key controls** with clear roles and responsibilities of the trustees and 3rd parties.
3. **Update the scheme's risk register** to include dedicated cyber risks as outlined in the risk assessment phase (e.g. data breach, systems outage, cyber enabled fraud), review the controls in place to manage these risks and the potential impacts and response steps if controls were to fail.
4. **Develop a vendor management framework** to consider your exposure to 3rd parties.
5. **Review the existing data breach incident response plan** against cyber best practice (guidance: https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes/developing-your-plan).
6. **Engage** with the corporate sponsor to align plans as far as possible.
7. **Review your risks and refresh your incident response plan periodically** (preferably annually).
8. **Keep up-to-date** with regular ongoing training.

Mercer

Marsh and Mercer are two of the Marsh & McLennan Companies, together with Guy Carpenter, and Oliver Wyman.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the “Marsh Analysis”) are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.

Registered in England and Wales Number: 1507274, Registered Office: 1 Tower Place West, Tower Place, London EC3R 5BU. Marsh Ltd is authorised and regulated by the Financial Conduct Authority for General Insurance Distribution and Credit Broking (Firm Reference No. 307511).

Mercer Limited is authorised and regulated by the Financial Conduct Authority Registered in England Mo. 984275 Registered Office: 1 Tower Place West, Tower Place, London EC3R 5BU

A business of Marsh McLennan

PENSIONS AND
LIFETIME SAVINGS
ASSOCIATION

# ANY QUESTIONS?

@ThePLSA

# Pension Schemes and Cyber Security: Practical Issues for Trustees

**Dan Boynton**

Shepherd & Wedderburn

PLSA Scotland Group - Cyber Security Winter Session

# Pension schemes and cyber security

Dan Boynton
Senior Associate, Shepherd & Wedderburn LLP

SHEPHERD+WEDDERBURN

# Agenda

- Cyber risks for pension schemes
- Legal and regulatory backdrop
- Practical issues
  - documentation
  - dealing with a cyber attack

- Focus on trustee perspective

# Main cyber threats

## Ransomware

- Encrypt data and demand ransom to unlock
- Stops use of systems:
  - members not paid?
  - unable to access investment choices
  - unable to invest employer contributions
- Route through malware and phishing (e.g. email attachments and links)

## Data theft

- Use of stolen identities
  - loan applications
  - other fraudulent purposes
  - sale on dark web
- Could be routed through malware

## Theft of assets

- Hack of pension systems
- Fraudulent disinvestment
- Fake invoices

# Impact on scheme

- Unable to provide service
- Regulatory response and potential fines
- Loss of data
- Dissatisfied members
- Claims/ compensation
- Reputational risk

# Trustee legal framework

## Data protection

- UK GDPR and DPA 2018 : Trustees as data controllers
- Securing personal data by appropriate technical and organisational measures
- Clearly documented policies and ongoing accountability
- Reporting obligations
- Scrutiny and potential fines if not meeting requirements

## Pensions Act 2004

- *"… must establish and operate an effective system of governance including internal controls"* S249A
- System proportionate to size, nature, scale and complexity of scheme activities
- *"These controls need to include measures to reduce cyber risk"* TPR, draft single code

## Wider fiduciary role

Protecting against cyber risk intrinsic to fiduciary role

# Regulatory framework

- Cyber security “principles” for pension schemes, TPR 2018 Guidance
- Can trace back to earlier statements (e.g. Lesley Titcomb, 2016)
- General Code: “cyber controls” module
- Status of guidance on adoption of general code?

*“Cyber security is a topic we have already addressed in [the principles]…*

*…however, survey data indicates that cyber security processes are still rare…*

*…to ensure that more schemes address this pressing issue, we have taken the opportunity to reinforce our guidance and place direct expectations on schemes…”*

**TPR consultation on draft single code**

# 2018 TPR guidance

## General

- Good practice processes to help Trustees tackle cyber risk and build resilience
- See cyber risks as part of the risk assessment cycle
  - understand risks
  - put controls in place
  - then consider and report on those controls regularly
- Building cyber resilience part of operating adequate internal controls

# 2018 TPR guidance

Other key points include:

- Clear roles and responsibilities
- Training
- Cyber risk should be on risk register and regularly reviewed
- Understanding of risk -Cyber footprint
- Third party supplier controls
- Incident response plan
- Expertise
- Clarity on reporting
- Evolving risk

# Draft Single/General code

- General code will include cyber module
  - Internal controls include measures to reduce cyber risk
  - Draft wording less detailed than in guidance, but “builds on” guidance
  - Further guidance to accompany code ?
- Greater emphasis on avoiding incidents plus managing those occur
  - Policies for the use of devices, and for home and mobile working.
  - Policies and controls on data in line with data protection laws
  - Policies to assess whether breaches need to be reported to ICO
- Cyber incident response plan

# Cyber policy documentation

- Individual or general policy? Can document everything in one place
- Shows Trustees properly thinking about cyber risk and have measures in place to adapt.

Use TPR guidance/code as framework to ensure expectations met, including :

- Responsibilities
- Descriptions of cyber crime
- How schemes could be vulnerable to attack/risk assessment/consequences
- Cyber crime prevention strategy: e.g. internal and external security measures (e.g. due diligence steps with external providers)
- Mitigating and managing the risks (e.g. training, technology solutions)
- Policies on working from home and mobile data use
- Include cyber-crime incident management plan – where attack involves personal security data breach, cross-refer to and invoke Data Protection Data Breach Management Policy.

# Dealing with risk in practice

## TPR cyber risk assessment cycle

### Assess and understand the risk

- Key functions, systems and assets
- Cyber footprint
- Risk register
- Access to right skills and expertise to understand and manage risk

### Put controls in place

- IT security controls, processes and people
- Assurance on third party provider controls
- Standards/accreditations
- Incident response plan
- Data protection compliance

### Monitor and report

- Controls, processes and response plans regularly tested and reviewed
- Clarity on how and when incidents would be reported to you and others (including regulators)
- Keeping regularly up to date on cyber risks, incidents and controls
- Keeping up to date with information and guidance on threats

# Third party providers

## Carry out appropriate checks

- Do providers meet best industry cyber security standards?
- Cyber controls module: ensure appropriate system controls in place
- Ask about cyber controls in new appointments
  - but may not be case for long-standing appointments.

## Practical issues

Questionnaires:

- Could have different approach based on risk:
  - administrator or investment adviser
  - non-administrator

Based on cyber footprint and potential impacts

- Assessing responses

# Dealing with a data breach

## Regulator reporting

**ICO: data breaches:**

- If any risk to members
- Trustees report without undue delay and within 72 hours of their awareness

**Members: data breaches:**

- If high risk to members – report without undue delay (e.g. identify theft risk).

**Pensions regulator - breach of law report:**

- Non-compliance of legal duty relating to scheme administration likely to be of material significance to TPR
- e.g. cannot operate pensions payroll due to cyber attack
- Breach of ESOG requirement ?

## Response to breach

- Incident response plan
- TPR public comments following Capita cyber incident, April 2023 : reporting expectation
- Trustees' data breach log

# Final thoughts

- Use of technology to administer schemes increased greatly
- See cyber along with other major scheme risks
- Under prepared schemes – position also for large corporate boards?
- Clearer expectations from TPR
- TPR public statements following recent Capita cyber security incident : reflect on how address cyber risk
- Need to draw together different sources of legal and regulatory requirements – dedicated project
- A few simple actions could have a big impact

SHEPHERD+ WEDDERBURN

shepwedd.com

**Edinburgh**
9 Haymarket Square
Edinburgh
EH3 8FY
T +44(0)131 228 9900

**Glasgow**
1 West Regent Street
Glasgow
G2 1RW
T +44(0)141 566 9900

**London**
Octagon Point
6th Floor, 5 Cheapside
London EC2V 6AA
T +44(0)20 7429 4900

**Aberdeen**
37 Albyn Place
Aberdeen
AB10 1YN
T: 01224 621166

**Dublin**
27/28 Herbert Place
Dublin
D02 DC97
E info@shepwedd.com

PENSIONS AND
LIFETIME SAVINGS
ASSOCIATION

# ANY QUESTIONS?

@ThePLSA

Cyber Security: Data and Compliance

# LUCY STONE

The Pensions Regulator

The Pensions Regulator

Making workplace pensions work

# TPR expectations

# What are the requirements in respect of cyber controls?

- Trustees and scheme managers have a requirement to operate adequate internal controls:
  - arrangements and procedures to be followed in the administration and management of the scheme
  - systems and arrangements for monitoring that administration and management
  - arrangements and procedures to be followed for the safe custody and security of the assets of the scheme.
- Cyber controls are just another form of internal control
- But it feels different – constantly evolving and unfamiliar
- Complements duties in data protection law
- Expectations outlined in guidance in 2018
  - Core principles being brought into general code.
  - Updated guidance to be published shortly

# Trustees' role

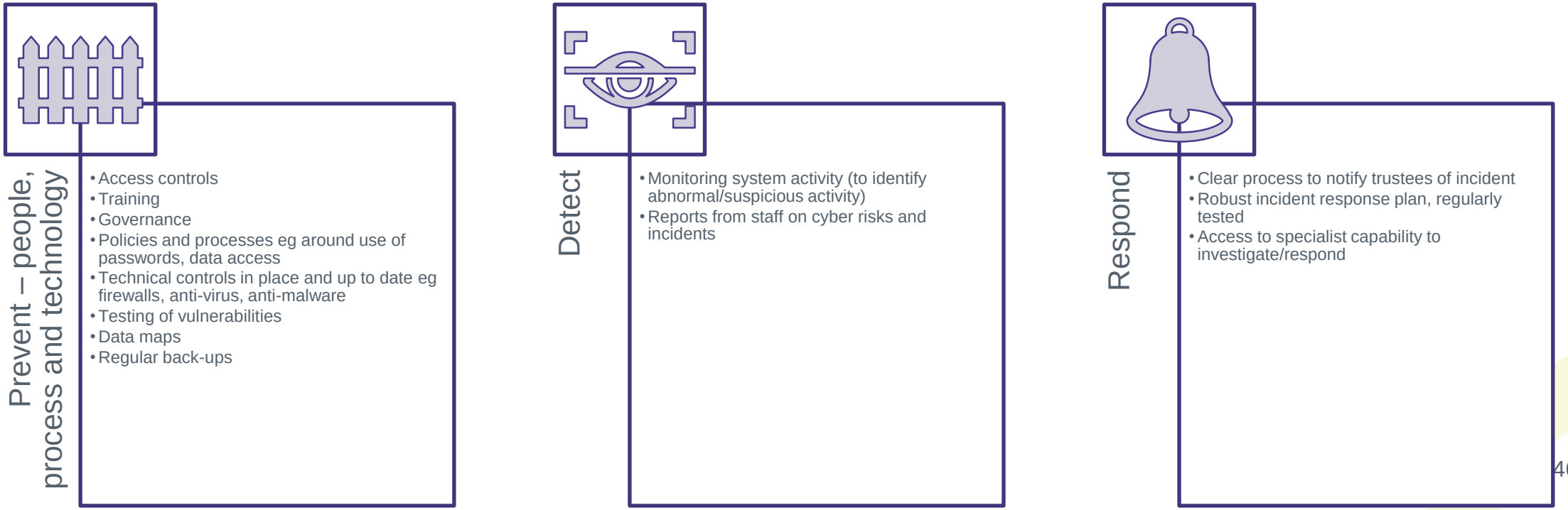
- Accountable, even though others handle data and manage technology on their behalf
- Exercise good governance:
  - Risk management – understand, prevent, respond
  - Oversight and management of service providers
- Complex and evolving risk needs a dynamic response – regularly test, review and update.

# Understand the risk

- What is the '**cyber footprint**' of your scheme – the digital presence of all the parties involved in your scheme?
  - Not just the administrator… but also employers, other advisors (auditor, actuary, investment manager, lawyer etc), members and of course trustees themselves!
- What are your **critical functions** and what **systems and assets (including data)** do you need to deliver these? What is their value to a criminal?
- **What incidents might these systems and assets face**? How vulnerable are they to cyber incidents?
  - Accidental disclosure, staff-related insider threats, hacking, malware, ransomware, phishing
- What is the **potential impact** of a cyber incident on your scheme, your members and (where appropriate) the sponsoring employer?
  - Operational, reputational, financial

# Ensure controls are in place

- **Assure yourselves that those handling data or managing technology on your behalf have sufficient controls in place** to reduce the risk of a cyber incident occurring, detect cyber incidents and respond effectively
- Controls **proportionate to your scheme and your cyber risk**. At a minimum, expect these to be in line with Cyber Essentials/10 steps to cyber security/cover the below.



# Incident response plan

Not if but when

- Clear roles and responsibilities
- Processes to be followed in case of cyber incident. Safety first!
  - Contain - shut down elements of your infrastructure to prevent malware and viruses from spreading
  - Swiftly determine which data has been compromised and who might be affected; and recover scheme records from backup.
  - Only bring systems and data back online when you are confident that they are secure
- Prioritised scheme services covering at a minimum, pensioner payments, retirement processing and bereavement services
- Internal and external comms plans
- Support services to members
- Report breaches to us and the Information Commissioner

For all those handling data and managing technology on your behalf, and trustees themselves

# What are we seeing?

- Increased focus on cyber and rising presence of controls, though still more likely to be in place in larger schemes
  - Understandable, but still need to take proportionate approach
- Growing presence of incident report plans but not universal
  - Preparedness AND resilience
- Overreliance on employers and administrators' plans, sometimes without scrutiny
  - And what about their suppliers?
- Administrators a key focus for trustees, but others (actuaries, lawyers) less so
  - Consider the whole value chain
  - Trustee training itself!
- Unclear on who and when to communicate to members
  - Trustee responsibility, though can delegate
  - Can take time to investigate and confirm a breach – but can reach out proactively and keep members updated as this takes place
  - Useful materials from ICO and NCSC which can be provided to members

PENSIONS AND
LIFETIME SAVINGS
ASSOCIATION

# ANY QUESTIONS?

@ThePLSA

Human Layer Security

# BRIAN TAYLOR

Hymans Robertson

HYMANS ROBERTSON

# Human Layer Security

## For PLSA Scotland

16 November 2023

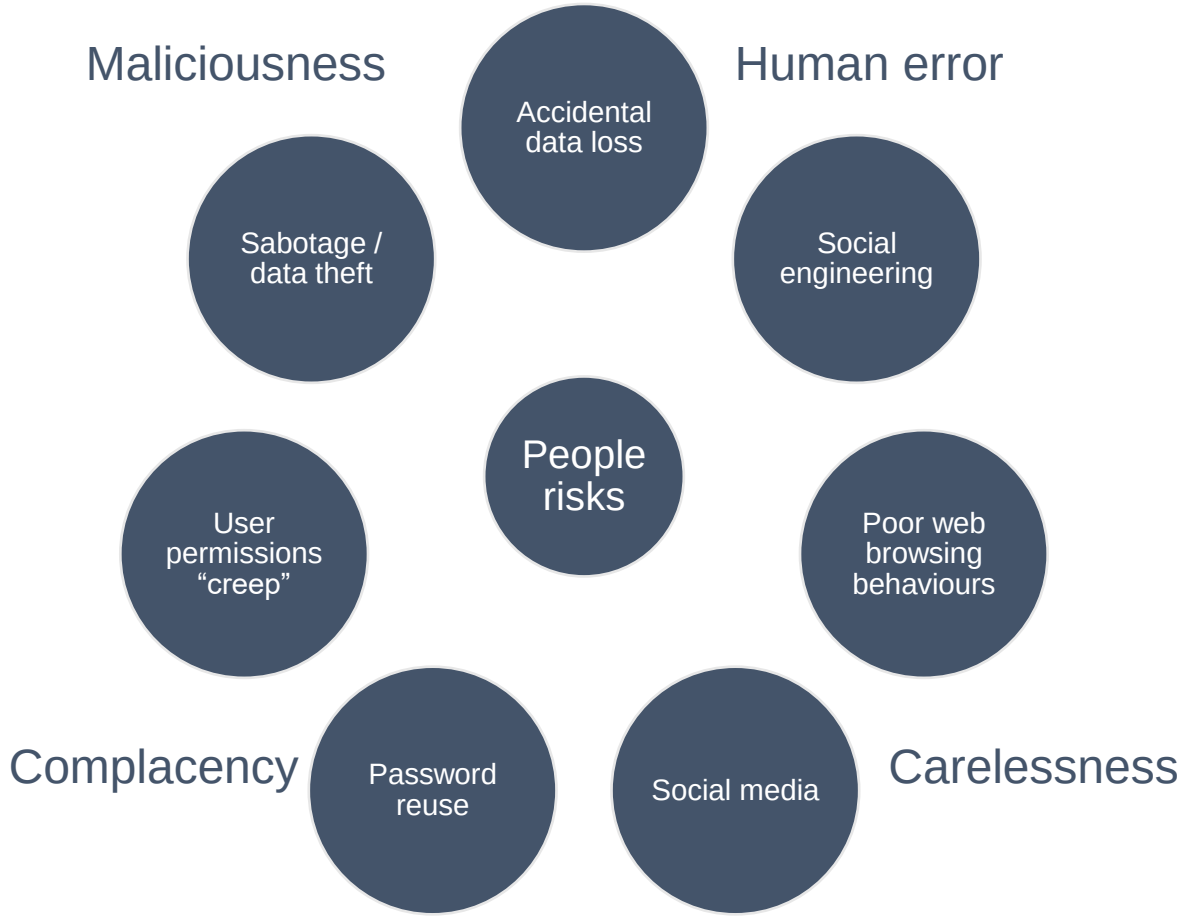
# Human Layer Security


- Human layer
- Data layer
- Application layer
- Endpoint layer
- Perimeter layer
- Network layer
- Physical layer

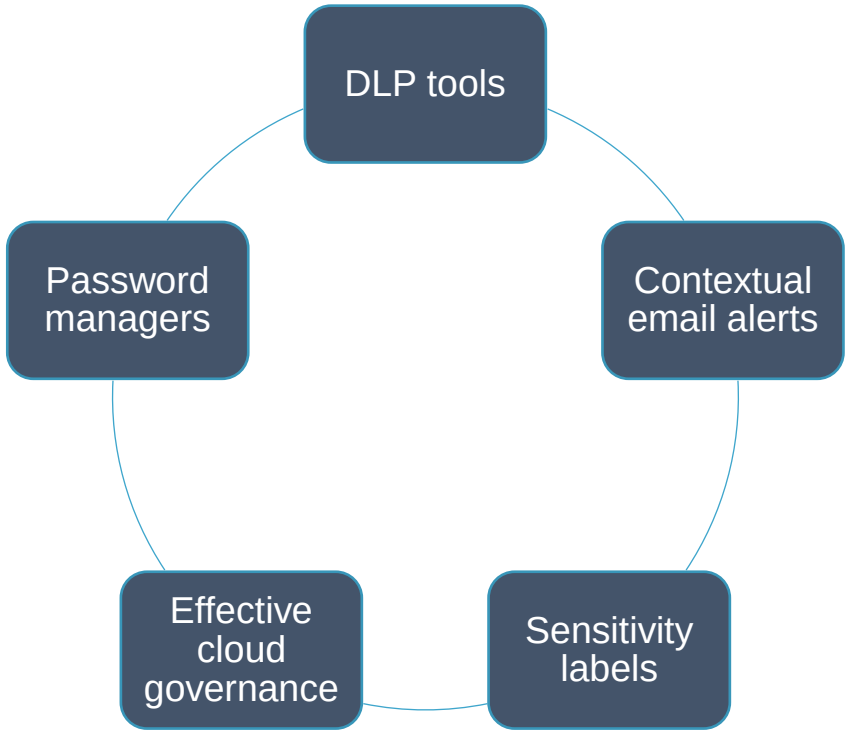
The human layer is the organisations' people and focuses on awareness, training, behaviours and understanding and securing interactions between people

Traditional security models have focused on technical controls – firewalls, spam filter, antivirus tools, identity management, encryption…

# Our people

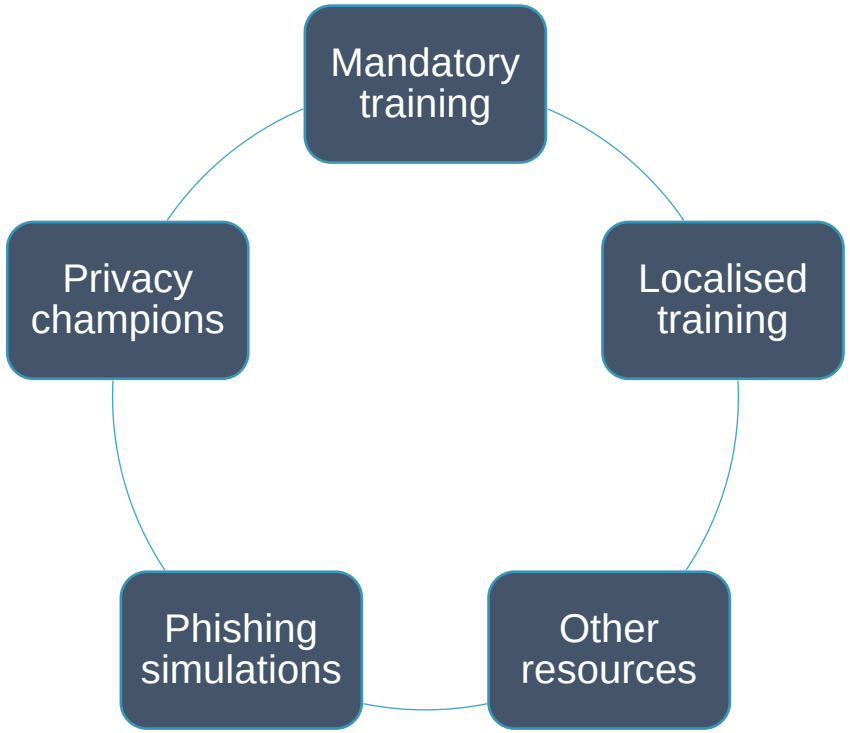



# Practicalities: Technology measures




- Detecting and warning about accidental (or deliberate!) data exfiltration
- Detecting and warning about possible misdirected email – e.g. odd combination of recipients
- Labelling documents and emails to prevent inappropriate sharing – e.g. internal use only
- Blocking or limiting data transfers to unauthorised cloud apps
- Encourage use of password managers to help avoid password reuse and credentials hacks

# Practicalities: Training and awareness




- Regular mandatory information security and data protection training
- Localised training, tailored to specific areas or functions
- Guidance and other materials available e.g. on the staff intranet
- Targeted phishing simulation exercises
- Privacy champions, who've had more in-depth training

# Psychological safety

“A shared belief held by members of a team that it’s OK to take risks, to express their ideas and concerns, to speak up with questions, and to admit mistakes — all without fear of negative consequences.”

- Harvard Business Review

# Speaker contact details


**Brian Taylor CIPP/E**

Head of Information Governance and Group Data Protection Officer

0131-656 5167

brian.taylor@hymans.co.uk

LinkedIn profile

HYMANS ROBERTSON

# Thank you

PENSIONS AND
LIFETIME SAVINGS
ASSOCIATION

# ANY QUESTIONS?

PLEASE USE THE Q&A BOX TO ASK QUESTIONS

@ThePLSA

PENSIONS AND
LIFETIME SAVINGS
ASSOCIATION

# SPEAKER PANEL

@ThePLSA

## FUTURE EVENTS

- ESG Conference: London, 29 November
- PLSA Policy Insights Webinar: 'The Regulatory Horizon' for 2024, 7 December
- LA Forum: London, 14 December

## NEXT MEETING DATE

- Scotland Group Meeting, 26 February 2024, Edinburgh

## PLSA 2024 CONFERENCES

- Investment Conference, 27-29 February, Edinburgh
- Local Authority Conference, 11-13 June, Gloucestershire
- Annual Conference, 15-17 October, Liverpool

Please visit www.plsa.co.uk/events to register

PENSIONS AND LIFETIME SAVINGS ASSOCIATION

# THANK YOU FOR ATTENDING THE SCOTLAND GROUP MEETING

@ThePLSA