Cyber Risk Training

Prepared for:	Cumbria Local Government Pension Scheme
Prepared by:	Jason Wilson and Chris Emmerson, Aon
Date:	15 July 2022

QAS Institute and Faculty of Actuaries®
Quality Assurance Scheme

Training Agenda

What we will cover today

1. **Knowledge and skills competencies**
2. **What is cyber security and risk**
3. **Current cyber threat trends**
4. **LGPS Response to cyber threats**
5. **Discussion/next steps**

CIPFA Knowledge and Skills Competencies – Cyber

Committee and Board

A **general understanding** of:

- the fund's **cyber security policy** (across all areas of Fund activity)
- how the pension fund **monitors and manages the performance of their external suppliers and providers**, including **cyber risk**

Senior Officers

An **expert knowledge** of the **cyber security** policy across all areas of fund activity

A **detailed knowledge** of how the fund monitors and manages the performance of its outsourced providers

What is cyber security and risk

What is Cyber Security and Cyber Risk?

Important definitions

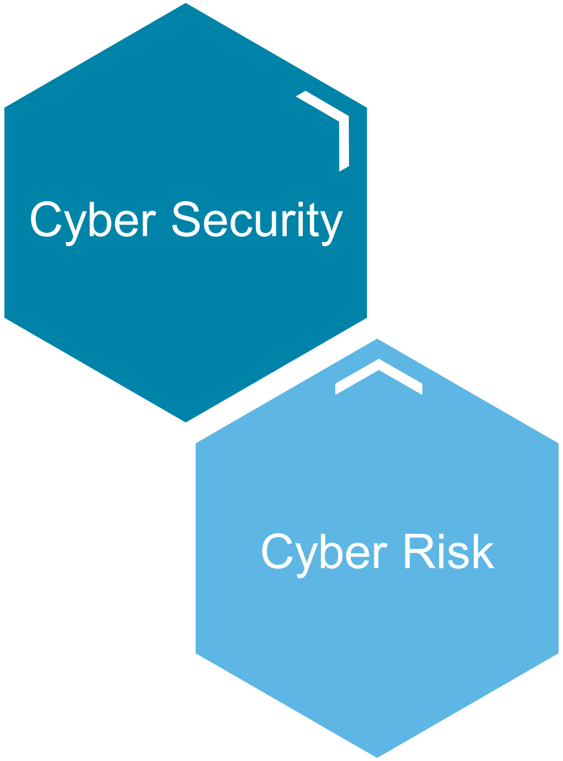
Cyber Security –

- The **protection of devices, services and networks** - and the **information** on them - from **theft or damage** via electronic means *(from the National Cyber Security Centre)*.

Cyber Risk –

- Can be broadly defined as the **risk of loss, disruption or damage** to a scheme or its members as a result of the failure of its information technology systems and processes.
- It includes **risks to information** (data security) as well as **assets**, and both **internal risks** (e.g. from staff) and **external risks** (e.g. hacking).

  (from the Pensions Regulator's Cyber Guidance).



Dispelling some cyber myths

1

Myth 1 – Cyber is complex – I won’t understand it

Reality: You don't need to be a technical expert to make an informed cyber security decision.

2

Myth 2 – Cyber attacks are sophisticated, I can't do anything to stop them

Reality: Taking a methodical approach to cyber security and enacting relatively small changes can greatly reduce the risk to your organisation.

3

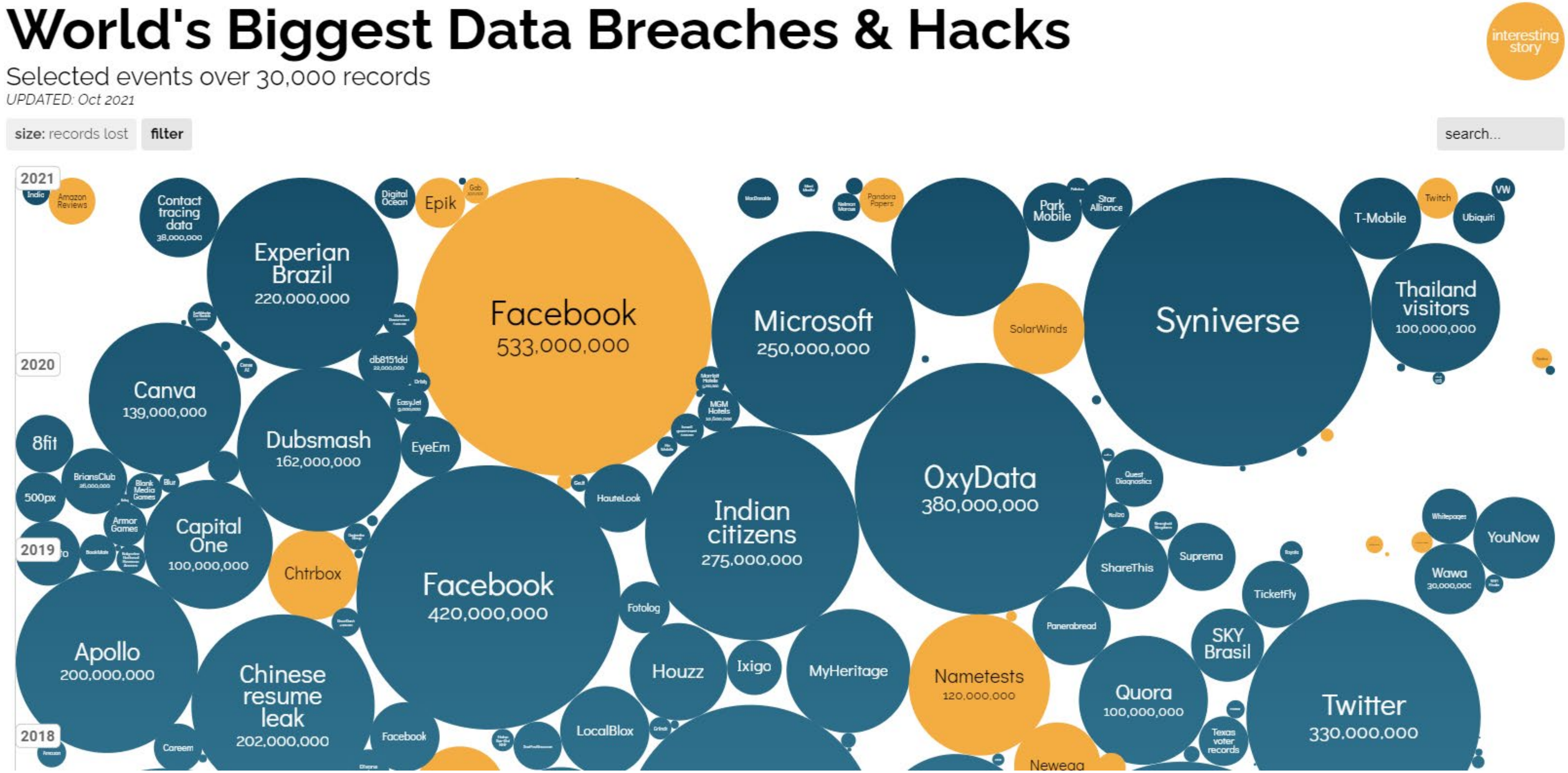
Myth 3 - Cyber attacks are targeted, I'm not at risk

Reality: Many cyber attacks are opportunistic and any organisation could be impacted by these untargeted attacks.

Source: National Cyber Security Centre

Current cyber threat trends

Cyber threat trends



World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED: Oct 2021

size: records lost

filter

search...

Source: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Where do the threats come from?

- Loss of hardware (laptop, mobile, USB)
- Loss of electronic data
- Computer systems failure

Accidental

- “Hobbyist” hacker
- Generic malware (e.g. WannaCry)

Untargeted

- Ex-employee (e.g. Snowden)
- Customer
- Current employee
- (Anonymous) Activist

Targeted

- Cyber criminal
- Competitor
- Cyber terrorist
- State-sponsored attack

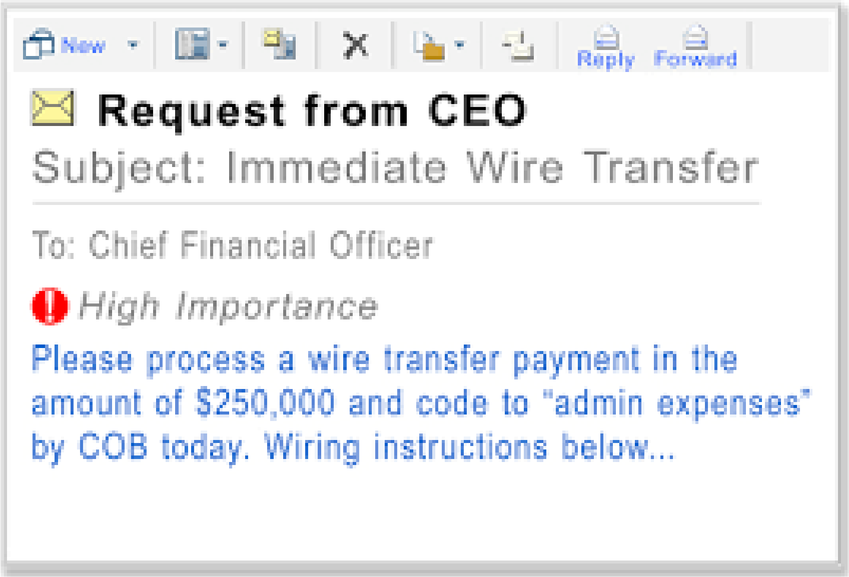
Severe

Key types of attacks

These include - **Business Email Compromises**, **Ransomware** and **Denial of Service**

Business Email Compromise

- Spoofed emails apparently from trusted sources request money transfers
- 400+ companies targeted per day globally
- $3 billion+ lost in past 3 years
- 40% of victims are Small & Medium Enterprises
- 14% of victims are in financial sector



Request from CEO

Subject: Immediate Wire Transfer

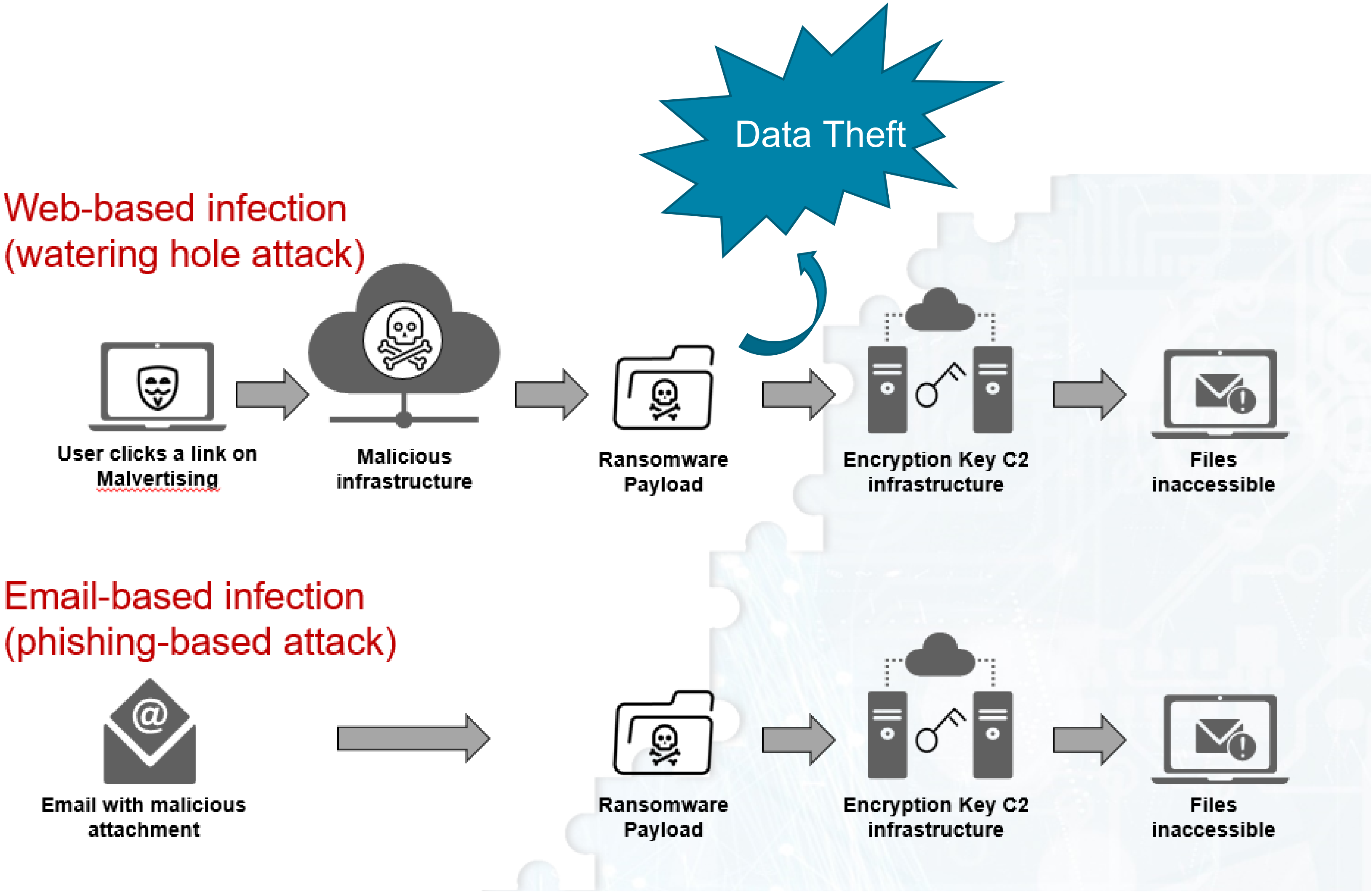
To: Chief Financial Officer

High Importance

Please process a wire transfer payment in the amount of $250,000 and code to "admin expenses" by COB today. Wiring instructions below...

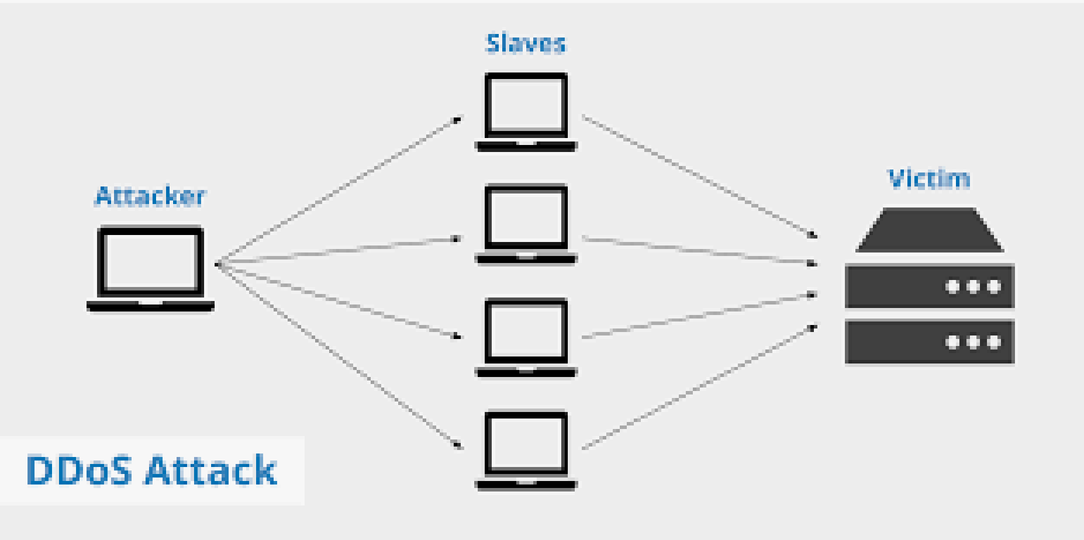
Source: fbi.gov

Ransomware


Data Theft
Web-based infection
(watering hole attack)
User clicks a link on Malvertising
Malicious infrastructure
Ransomware Payload
Encryption Key C2 infrastructure
Files inaccessible
Email-based infection
(phishing-based attack)
Email with malicious attachment
Ransomware Payload
Encryption Key C2 infrastructure
Files inaccessible

Distributed Denial of Service (DDoS)

- Botnet overwhelms target systems with traffic
- Systems unable to function normally
- Motives: Extortion, hacktivism, disruption, revenge, distraction



Source: keycdn.com

Cyber security in the pensions environment

Pension scheme threats

UK exposures

£2 trillion of pension scheme assets[1]

39 million members[2]

At least **50 million** separate records[3].

30,000 pension scheme trustees[4]

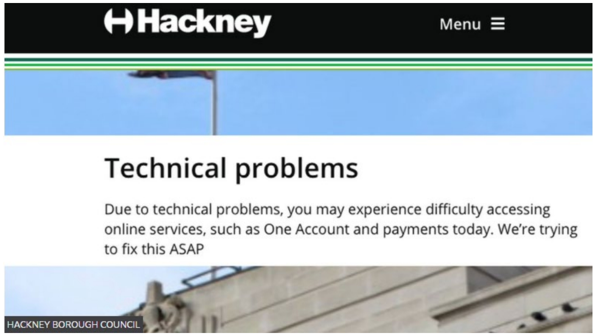
[1] Source: OECD Pension Market focus 2017 edition

[2] Source: Occupational Pension Schemes Survey: UK, 2016

[3] Source: Occupational Pension Schemes Survey: UK, 2016

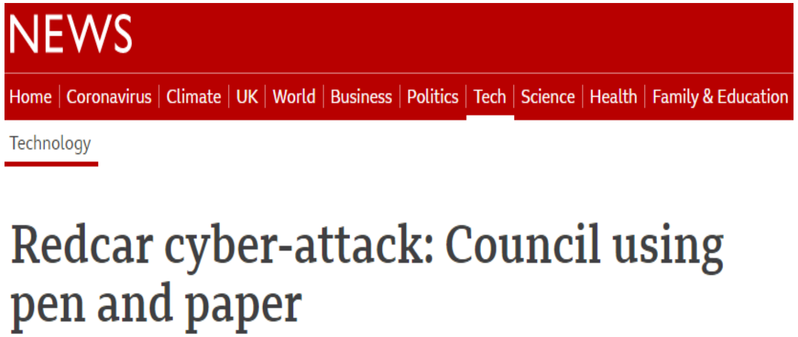
[4] Source: Estimated from The Pensions Regulator Trustee Landscape Quantitative Research 2015 and Scheme Return data

Threats becoming real

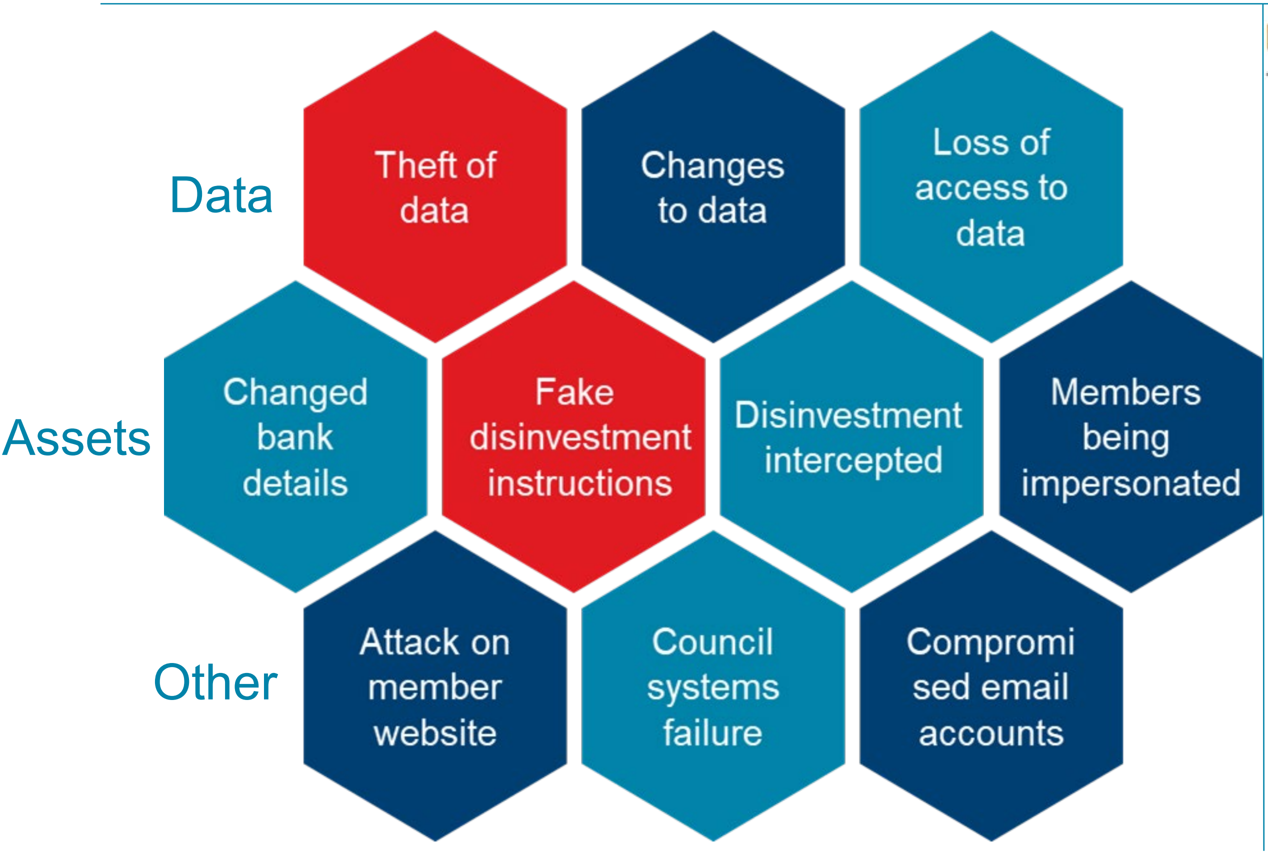


Technical problems

Due to technical problems, you may experience difficulty accessing online services, such as One Account and payments today. We're trying to fix this ASAP


NEWS
Home | Coronavirus | Climate | UK | World | Business | Politics | Tech | Science | Health | Family & Education
Technology

Redcar cyber-attack: Council using pen and paper



Data

Theft of data

Changes to data

Loss of access to data

Assets

Changed bank details

Fake disinvestment instructions

Disinvestment intercepted

Members being impersonated

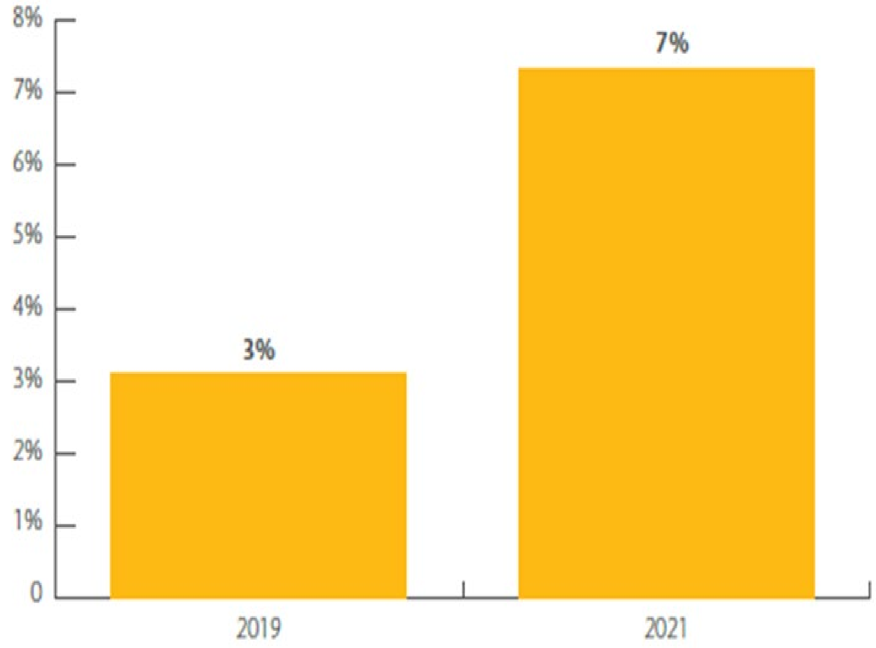
Other

Attack on member website

Council systems failure

Compromised email accounts

Proportion of schemes impacted by cyber incident



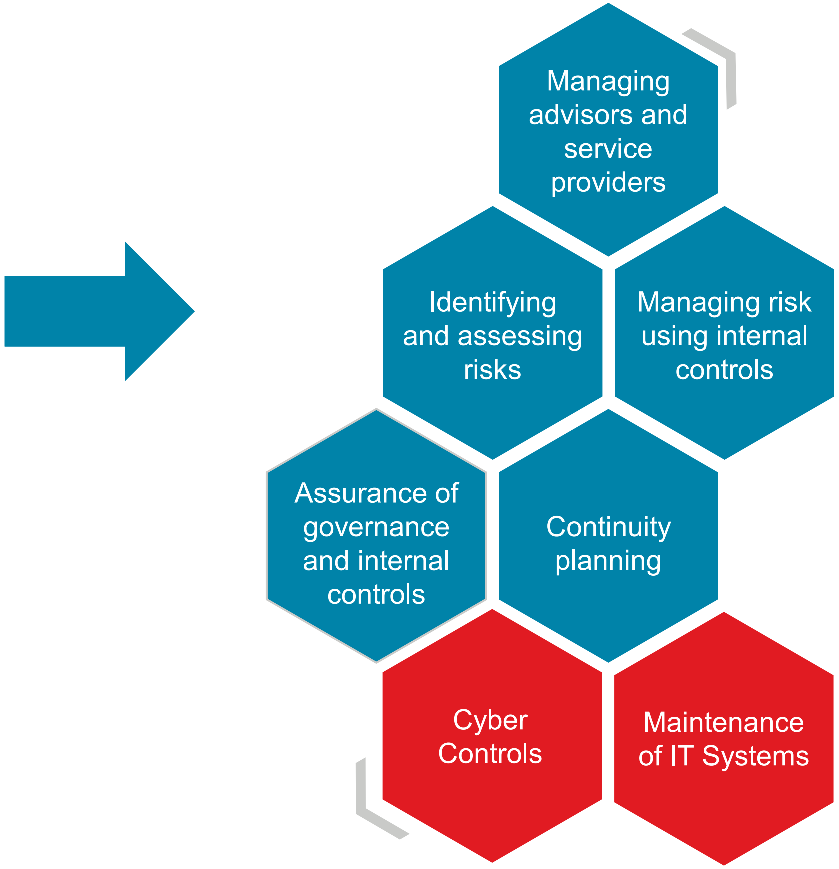
Source: *Aon Global Risk Survey 2021*

The Pensions Regulator – landscape

2018 Guidance

- Roles and responsibilities should be clearly **defined, assigned and understood**
- Cyber risk should be on your scheme's **risk register** and regularly reviewed
- You should have access to the **required skills and expertise** to understand and manage the cyber risk in your scheme
- You should ensure sufficient understanding of cyber risk: your scheme's key functions, systems and assets, its '**cyber footprint**', vulnerabilities and impact
- You should ensure **sufficient controls** are in place to minimise the cyber risks
- You should assure yourselves that all **third party suppliers** have put sufficient in place
- There should be an **incident response plan** in place to deal with incidents and enable the scheme to swiftly and safely resume operations
- You should be clear on how and when **incidents would be reported** to you and others, including regulators.

2022 Single Code


Managing advisors and service providers
Identifying and assessing risks
Managing risk using internal controls
Assurance of governance and internal controls
Continuity planning
Cyber Controls
Maintenance of IT Systems

Don't forget – legal requirements relating to internal control

Managing cyber risk is a key element of risk management and managing internal controls

The Pensions Regulator – Cyber insight

2019 TPR Statement

“It is important that scheme managers recognise, and maintain, a separation between the fund and Local Authority to **avoid an over-reliance on the Local Authority’s [cyber] policies and procedures**.”

2020/21 TPR Public Service Survey

- 90% of Public Service Schemes have at least half of TPR’s 14 cyber controls
- 1/3rd experienced some kind of cyber breach or attack

Cyber controls in new Single Code of Practice

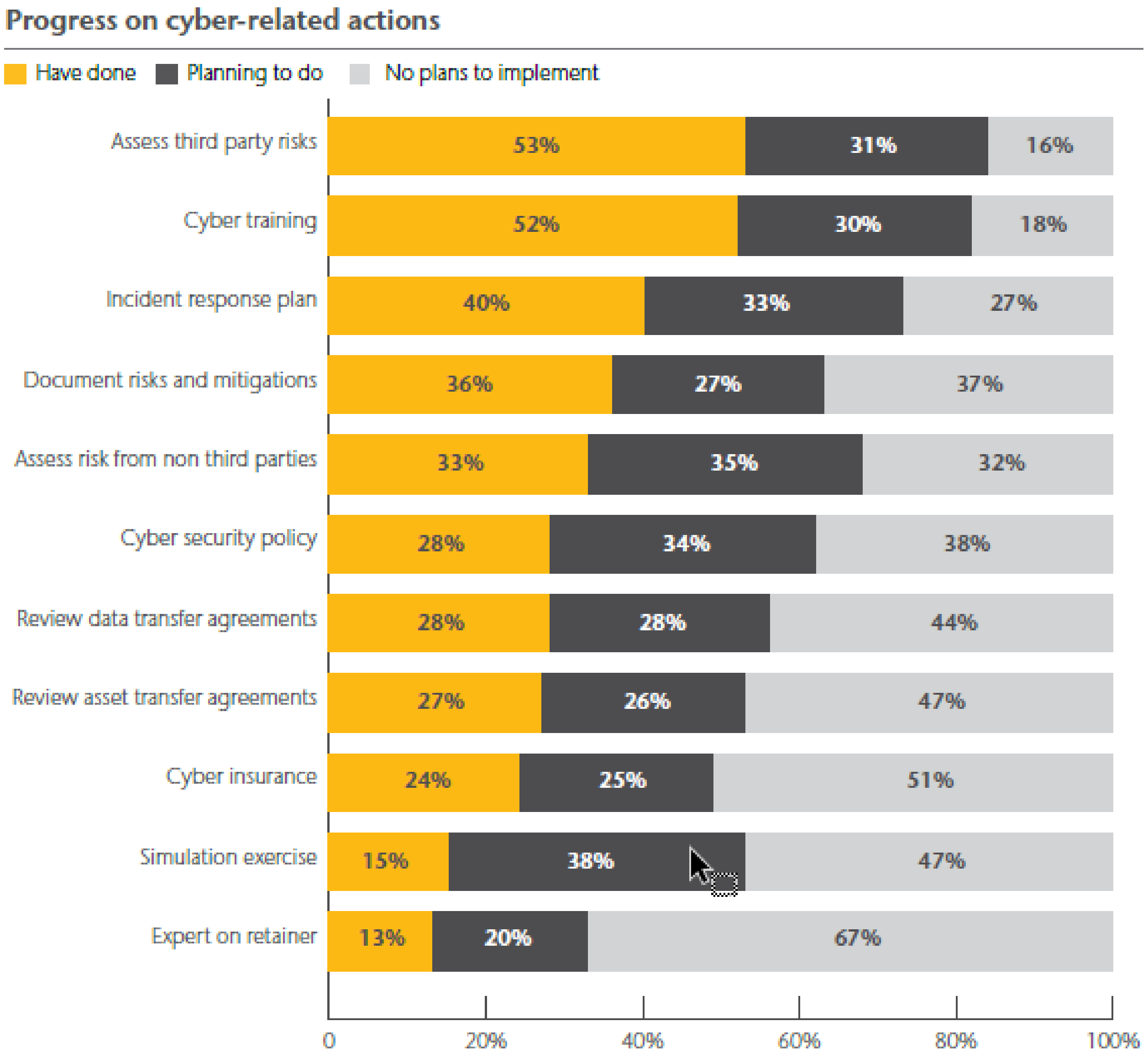
Key Points

- Fund policies, including
  - Data breach protocols
  - Cyber Incident response plan
- Review service provider controls
- Assess, at appropriate intervals, the vulnerability to a cyber incident

Further information

New Code of practice (still draft): https://www.thepensionsregulator.gov.uk/-/media/thepensionsregulator/files/import/pdf/full-draft-new-code-of-practice.ashx

Increased scheme activity



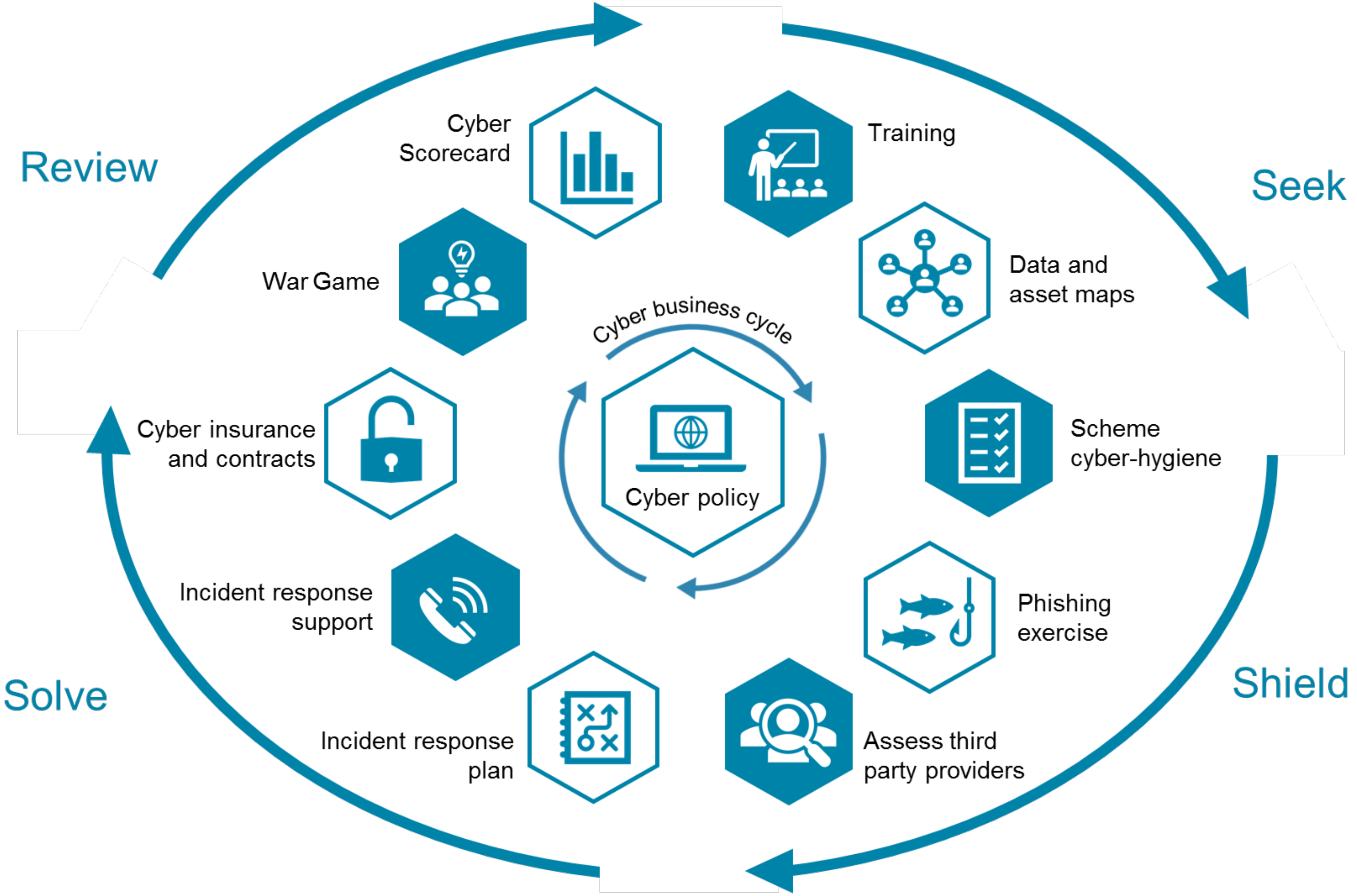
Source: Aon Global Pension Risk Survey 2021

Headlines

- Schemes have started to take actions but progress has been slow
- Significant increase in the number of schemes with an incident response plan
- Other common actions include assessing third party providers and documents risks and mitigations
- No correlation between the size of scheme and how much they have done

LGPS response to Cyber threats

Cyber security policy



Source: Aon

Shield - Fund Cyber-hygiene

Passwords

- Do not repeat passwords on different sites
- Use long passwords – preferably passphrases.
- Include numbers, letters and symbols in your passwords
- Don't use passwords that are easy to guess e.g. date of birth

Multifactor authentication

- Switch on multifactor authentication, wherever available.

Device security

- Keep antivirus software and apps up to date.
- Use public Wi-Fi with caution
- Look for the lock icon in the URL bar when using the internet.

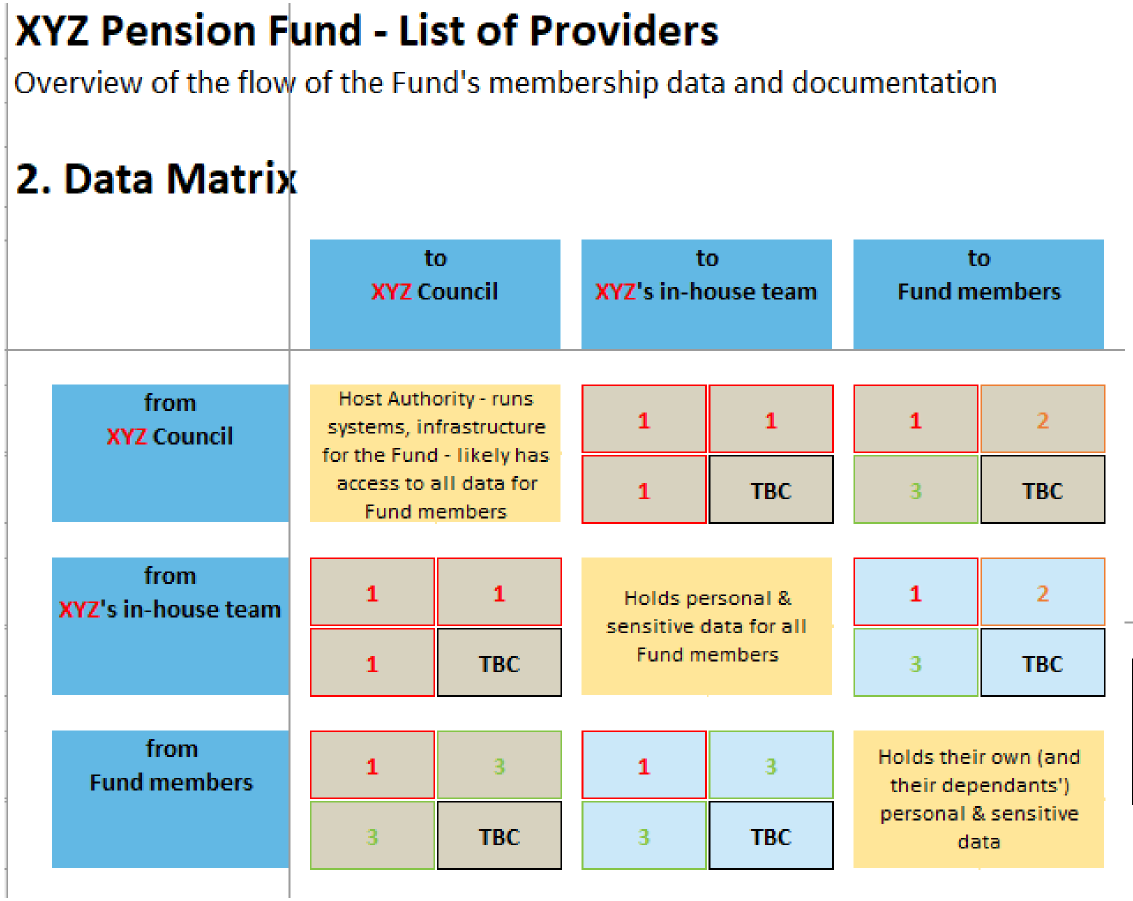
Be alert to scams

- Phishing still the most popular method
- Report suspicious emails.

Review social media footprint

- Review what information you and those connected to you post online and consider what information this could divulge.
- Report suspicious messages, links and activity

Seek - How does your data and assets move around?

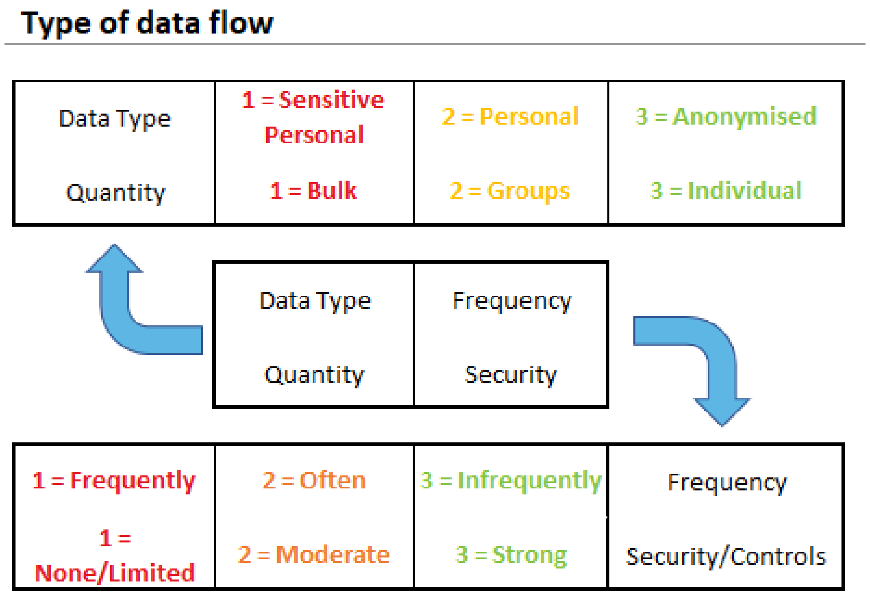


XYZ Pension Fund - List of Providers

Overview of the flow of the Fund's membership data and documentation

2. Data Matrix

	to XYZ Council	to XYZ's in-house team	to Fund members
from XYZ Council	Host Authority - runs systems, infrastructure for the Fund - likely has access to all data for Fund members	1 1 1 TBC	1 2 3 TBC
from XYZ's in-house team	1 1 1 TBC	Holds personal & sensitive data for all Fund members	1 2 3 TBC
from Fund members	1 3 3 TBC	1 3 3 TBC	Holds their own (and their dependants') personal & sensitive data



Type of data flow

Data Type Quantity	1 = Sensitive Personal 1 = Bulk	2 = Personal 2 = Groups	3 = Anonymised 3 = Individual

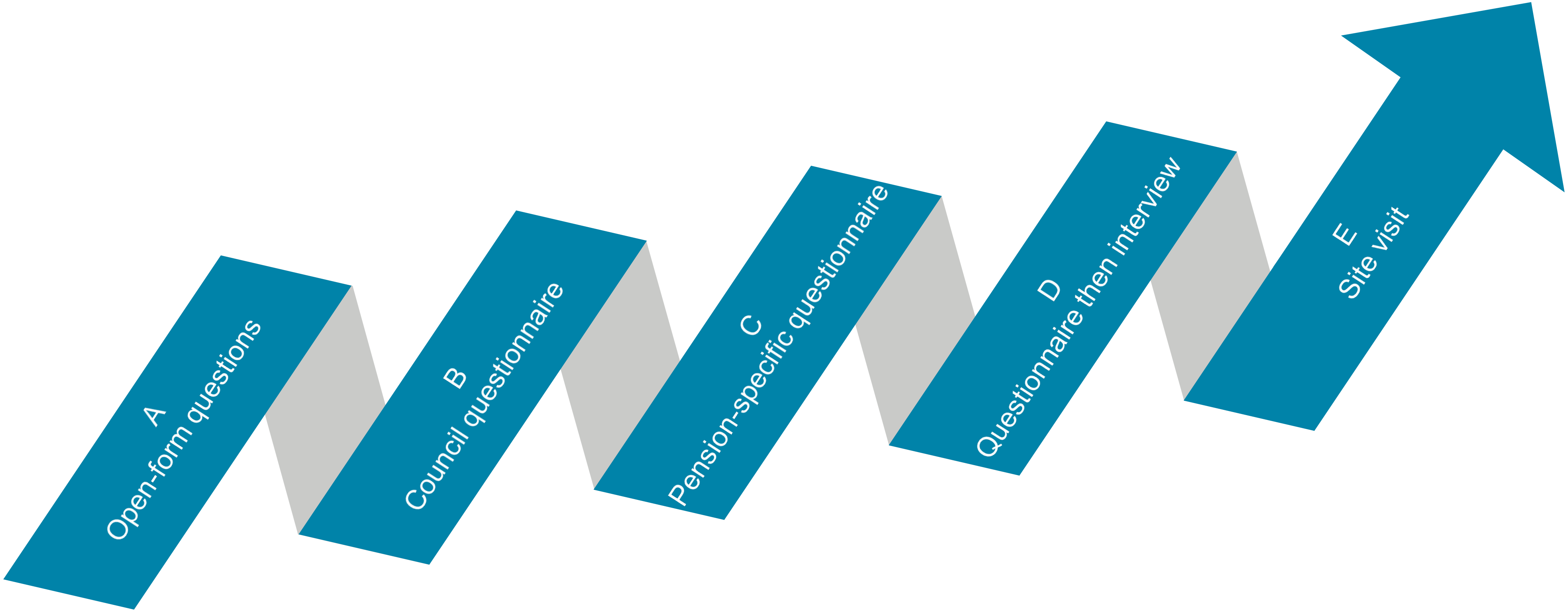
Data Type Quantity	Frequency Security

1 = Frequently 1 = None/Limited	2 = Often 2 = Moderate	3 = Infrequently 3 = Strong	Frequency Security/Controls

Seek

Understand and quantify the risk

Shield - How to assess third party providers



Open-form questionnaire

Simplest approach.

Each party asked how they deal with cyber risk.

Council questionnaire

Relatively common where host authority is large with good existing cyber awareness

Pension-specific questionnaire

Tend to be better tailored to Fund risks

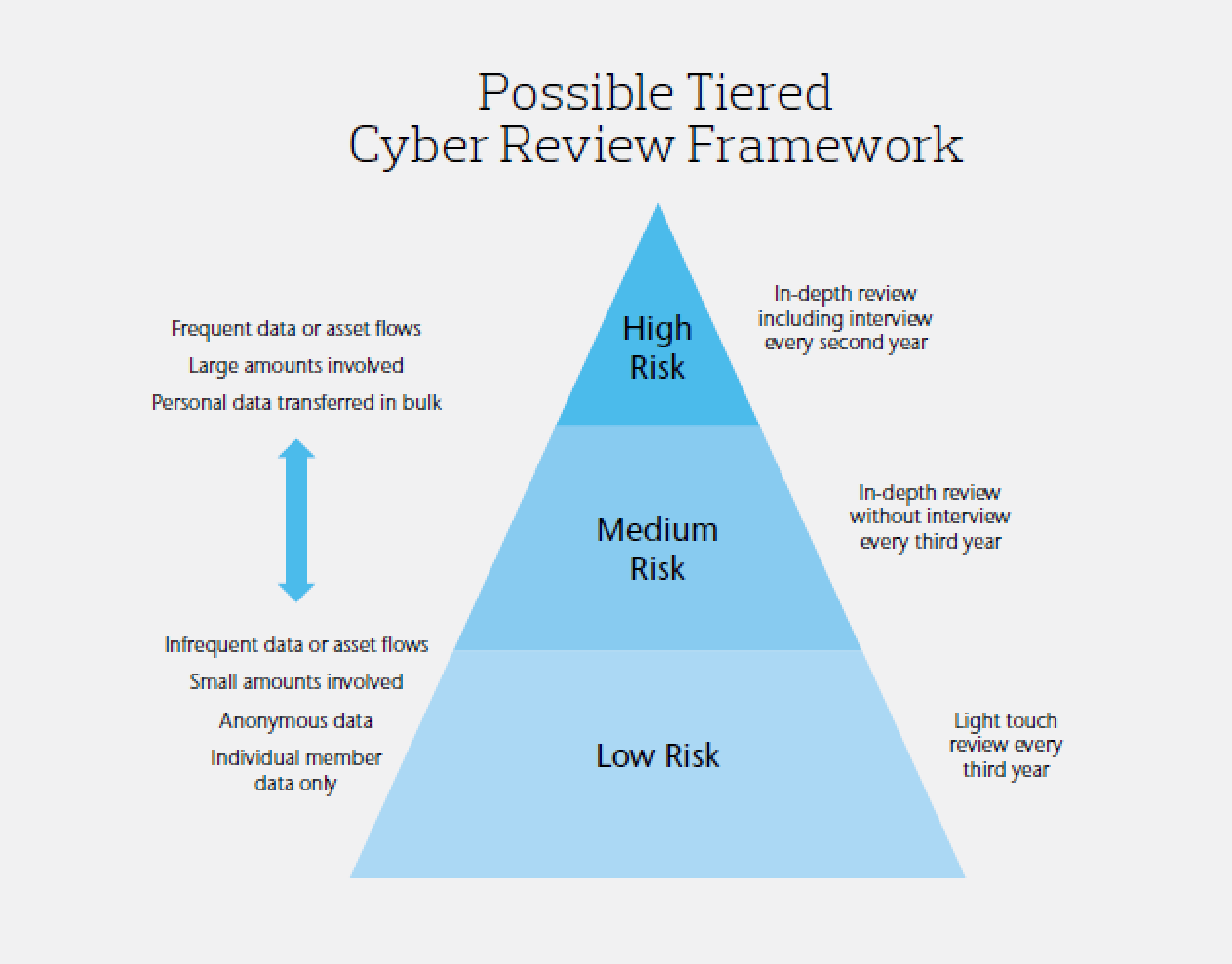
Questionnaire then interview

Cyber expert interviews day-to-day contact plus IT supplier to probe on questionnaire responses

Site Visit

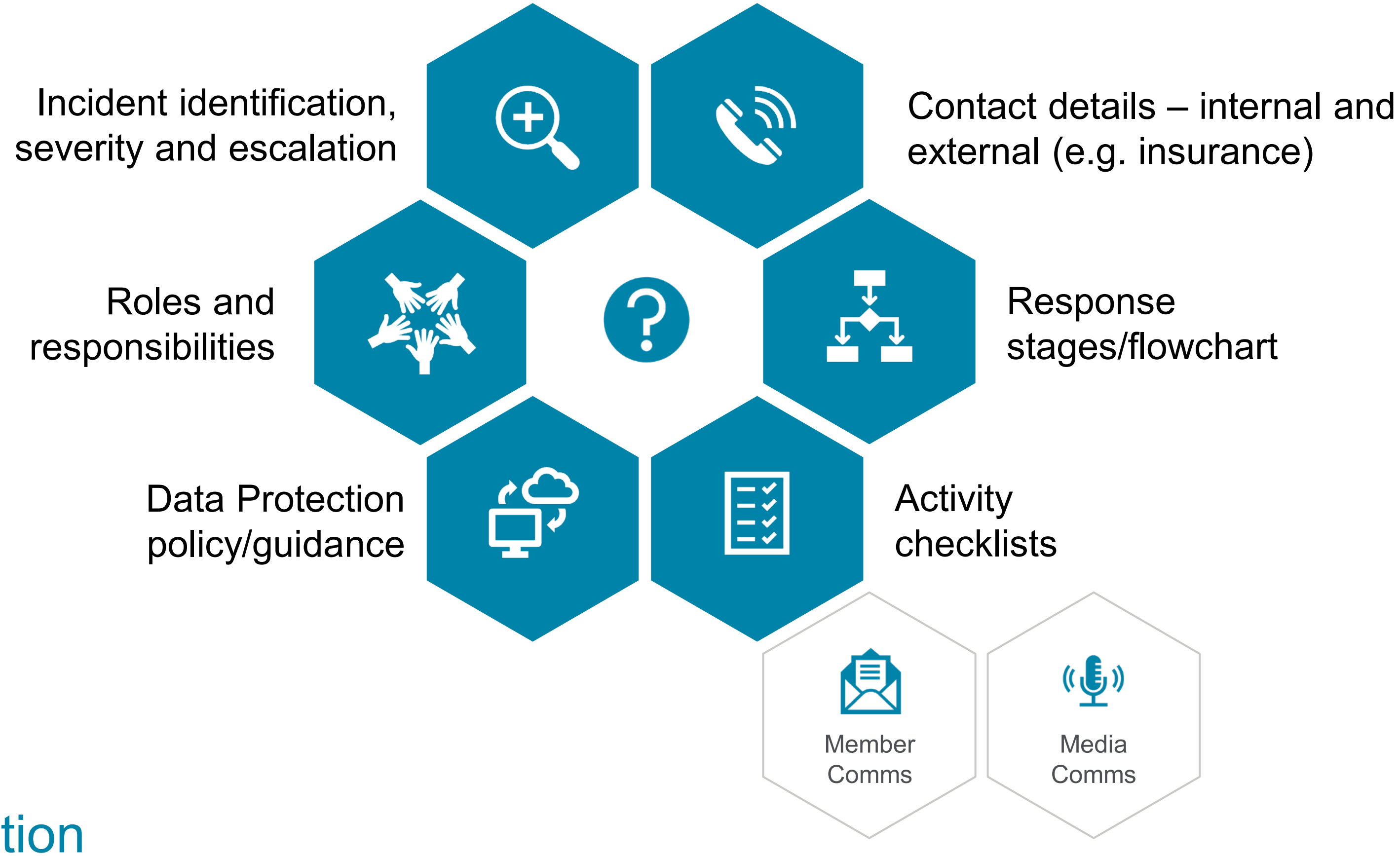
Extension of D to include a full site visit

Tiered cyber review framework



Possible Tiered
Cyber Review Framework
Frequent data or asset flows
Large amounts involved
Personal data transferred in bulk
High Risk
In-depth review including interview every second year
Medium Risk
In-depth review without interview every third year
Infrequent data or asset flows
Small amounts involved
Anonymous data
Individual member data only
Low Risk
Light touch review every third year

Solve - Incident Response Plan


Incident identification, severity and escalation
Contact details – internal and external (e.g. insurance)
Roles and responsibilities
Response stages/flowchart
Data Protection policy/guidance
Activity checklists
Member Comms
Media Comms

Action

Identify what incident response support is available: Internal expertise, from participating employers, insurance, expert on retainer

Questions and discussion

Jason Wilson
Senior Consultant
+44 (0) 207 864257
Jason.Wilson@aon.com

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

Aon Solutions UK Limited is authorised and regulated by the Financial Conduct Authority.
Registered in England & Wales No. 4396810
Registered office: The Aon Centre | The Leadenhall Building | 122 Leadenhall Street | London | EC3V 4AN

This document and any enclosures or attachments are prepared on the understanding that they are solely for the benefit of the addressee(s).
Unless we provide express prior written consent no part of this document should be reproduced, distributed or communicated to anyone else and, in providing this document, we do not accept or assume any responsibility for any other purpose or to anyone other than the addressee(s) of this document. In this context, "we" includes any Aon Scheme Actuary appointed by you.
To protect the confidential and proprietary information included in this document, it may not be disclosed or provided to any third parties without the prior written consent of Aon Solutions UK Limited.