THE MEMBER BACKING PENSIONS AND LIFETIME SAVINGS ASSOCIATION

*June 2022*

# CYBER RISK

## MADE SIMPLE GUIDE


## ACKNOWLEDGEMENTS

We would like to thank Aon and Crowe for their help in producing and sponsoring this guide. For further information visit

**www.aon.com** **www.crowe.co.uk**


Read all of our Made Simple Guides online at
https://www.plsa.co.uk/Resources/Made-Simple-guides
or scan the QR code below

This guide is for information only.
It is not legal or investment advice.


Published by the Pensions and Lifetime Savings Association 2021

# CONTENTS

# FOREWORD

## CYBERCRIME CONTINUES TO BE A REAL AND GROWING THREAT AROUND THE WORLD. COMPANIES AND GOVERNMENTS RECOGNISE THE RISK AND DEAL WITH THE CHALLENGES EVERY DAY. THERE'S NO REASON THAT PENSION SCHEMES SHOULD BE IMMUNE TO THE SAME THREAT – AND, INDEED, THE STATISTICS SHOW THAT THEY AREN'T.

At Aon and at Crowe we recognise the challenges that pension schemes face in relation to cybercrime. Those challenges come not only from the cyber risk itself, but from a range of other factors too:

- The unfamiliar nature of that risk to pension professionals and trustees
- The unique structures within which pension schemes operate
- The impact of the risk on the sponsor and members
- The limited resources that some schemes have to dedicate to this risk.

Using the cyber expertise within our respective businesses, combined with our in-depth understanding of UK pension schemes, Aon and Crowe have both developed cyber solutions specifically for UK pension schemes.

This Made Simple Guide reflects our expertise and our practical experience. We hope it provides a good starting point for schemes beginning their cyber journey, as well as suggested actions for schemes that have progressed further along the way.

**Paul McGlone**
*Partner*
Aon

**Jim Gee**
*Partner, National Head of Forensic Services*
Crowe

# 1. INTRODUCING CYBERCRIME

## A 21ST CENTURY PROBLEM

### CYBERCRIME IS THE PROBLEM OF OUR AGE, AND IT'S MADE WORSE BY THE FACT THAT THE NATURE OF THE PROBLEM CHANGES AND DEVELOPS WITH AN EVER-INCREASING SPEED.

It affects organisations from every sector, and pensions organisations are no exception. A key factor in this is their attractiveness to the cybercrime 'businesses' which are involved. This is both because of the large amounts of personal and financial data which they control, and because of the importance of continuing to pay pensions. Cybercriminals know that if they could carry out a ransomware attack which encrypted pensions data, the pressure to pay the ransom demanded would be enormous.

The development of small and medium-sized cybercrime 'businesses' into national and international ones over the last decade or so, along with their growth and profitability, has led to phishing becoming hugely more sophisticated and targeted than it was at its inception 20 years ago. Ransomware also continues to develop very quickly, with cybercriminals even using version numbers to ensure they use programs which as yet have no countermeasures.

When these 'businesses' look at government statistics on the prevalence of cybercrime – now representing more than 50% of all crime in the UK, with incidents increasing by over 110% since COVID and almost two-thirds of medium and large organisations suffering cyber breaches in 2020 – they are massively encouraged for the future and confident in the effectiveness of their 'business' model. Thirty-nine pension schemes reported actual cybercrime-related breaches (not just attacks) to the Information Commissioner's Office between April and November 2020.

It's important to clearly define a problem if it's to be tackled effectively. Cybercrime is not fraud, which is a different issue with different solutions.

When a computer is used to undertake fraud (as is often the case today) this is cyber-enabled fraud, not cybercrime. Cybercrime involves illicit intrusions into computers and networks (hacking) and/or the disruption of computer functionality, by means such as malware, ransomware and distributed denial of service ('DDoS') attacks. Data stolen through cybercrime can then be used for fraudulent purposes.

Two main cybercrime techniques are 'phishing' and the insertion of ransomware into a computer.

**Phishing** has been around for many years. It has been defined as 'the dishonest attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication'.

Phishing has become much more sophisticated in recent years, so it now includes:

- **Spear phishing**: the sending of targeted emails, directed at a specific individual rather than being sent randomly to multiple recipients (often preceded by research on the recipient)
- **Clone phishing**: the altering of previously sent (legitimate) emails to include new (illegitimate) links, with the intention that familiarity will trigger the opening of the email
- **Whaling**: a form of spear phishing targeted at celebrities and senior executives
- **Link manipulation**: the use of similar-looking URL links (for example: the real www.abcbank.com/customerservices might be changed to the fake www.abcbank.customerservices.com)
- **Filter evasion**: the sending of a photo or video which when clicked requires the victim to provide their email and password
- **Website forgery**: the development of similar but fake websites, which can infect the victim's computer
- **Covert redirect**: this typically occurs through the use of illegitimate pop-ups on legitimate websites which can infect the victim's computer
- **Vishing**: voice phishing. This can now be quite sophisticated, for example commonly available apps can be used to alter the number appearing to be that of the caller, alter the caller's voice, and add background office or other noise so the caller appears genuine.

**Ransomware** can encrypt the victim's files, making them inaccessible, and result in a demand for a ransom payment to decrypt them. By the end of 2021 ransomware attacks on businesses were taking place every 11 seconds.

However, ransomware can also be non-encrypting. It can involve the loading of pornographic images on to computer screens, or require the reinstallation of Windows software – both of which can only be avoided in return for the payment of a ransom. Mobile ransomware is used to display a blocking message over the top of all other applications for Android phones, and to use the Find My iPhone system to lock access to an iPhone.

Ransomware is particularly dangerous when deployed against organisations with a vital function, such as pension schemes, because the inability to perform that function can lead those running it to be tempted to pay the ransom. The National Cyber Security Centre (NCSC) supports the National Crime Agency (NCA) advice not to pay a ransom, as there's no guarantee you'll get access to your device (or data). Also, being known to have paid a ransom makes the victim more attractive to other cybercriminals.

**The Dark Web** is World Wide Web content (a series of 'darknets') which requires specific software, configurations or authorisation to access. It forms a small part of the Deep Web, the part of the Web not indexed by search engines.

It's a marketplace for illegal goods such as drugs and weapons. However, it's also used by cybercriminals to target organisations. Cybercrime tools, consultancy and compromised email accounts (with their passwords) are all for sale.

The Dark Web is where most cybercrime is organised and monetised. Research has revealed extensive discussions about attacking leading UK organisations, and how to monetise the attacks.

## CONCLUSION

Cybercrime is a complex, rapidly evolving phenomenon where specialist skills are needed to ensure proper levels of protection. To be able to provide the right quality of advice, advisers need to be immersed in the issue: The Pensions Regulator's (TPR) forthcoming new Code of Practice highlights the importance of such specialist skills and expertise to understand and manage cyber risks.

### ACTION 1: SPECIALIST SKILLS

**Trustees should review whether they have access to genuinely specialist advice concerning how to properly protect their pension schemes.**

# 2. CYBER FRAMEWORK FOR PENSION SCHEMES

## REGULATORY REQUIREMENTS

### FOR A PENSION SCHEME CONSIDERING CYBER RISK FOR THE FIRST TIME, IT CAN BE HARD TO KNOW WHERE TO START. IT IS A RISK THAT MOST TRUSTEES ARE NOT FAMILIAR WITH.

For many schemes the initial reaction can be that cyber risk is about data and administration, perhaps that it is very similar to General Data Protection Regulations (GDPR) issues. Of course, most schemes considered GDPR in detail in 2016, and have some data mapping, a data breach policy, and a broad understanding of their obligations to the Information Commissioner's Office (ICO) in the event of a data breach.


But while there are undoubtedly overlaps, cyber risk and GDPR are very different issues. There are GDPR issues that have nothing to do with cyber risk (e.g. rules around the processing of data) and there are cyber issues that have nothing to do with GDPR (e.g. system failures or asset losses).

Until recently, for most schemes the only regulatory requirement specifically relating to pension scheme cyber risk was TPR's Guidance from April 2018. At just a few pages long it is a good introduction to cyber risk, and a must-read for any trustee; but while it highlights issues for schemes to consider, it is short on real practical steps.

For DC Master Trusts the regulatory environment is more structured, with Code of Practice 15 (issued later in 2018) expanding on that Guidance.

But the biggest change is taking place this year: the introduction of TPR's Single Code of Practice. The new single code has a section specifically on cyber risk, as well as mentioning cyber risk in various other places. While the detail is in many ways similar to what was included in the 2018 Guidance and the Master Trust Code, the major change is that requirements around managing cyber risk are now being adopted in a formal Code of Practice for all schemes, rather than in a less formal guidance note. In effect, actions relating to cyber risk have been promoted from 'should probably think about' to 'should almost certainly do'.

## YOUR OWN FRAMEWORK

While the regulatory guidance is a good starting point, most schemes find that they need their own framework to translate those requirements into specific actions. Both Aon and Crowe use a similar framework when advising clients, and that is reflected in the structure of this guide:

- **Assess** – Chapter 3 explains how cyber risk can be assessed, as understanding the specific risks your scheme is exposed to, and existing vulnerabilities, is essential before you can better protect yourself.
- **Protect** – Chapter 4 explains how to reduce the risk that your scheme is exposed to, with practical actions you can take in a number of areas.

- **Respond** – Chapter 5 explains how you can be best prepared to respond and recover should an incident occur, and how you ensure you are still able to fulfil your key duties.
- **Governance** – Chapter 6 looks at the governance around your risk management process, including how it is documented and how you know the process is working as it should.

Many schemes adopt a similar framework within which they can place the actions that they are taking, or use a variation of a framework adopted by their sponsor. Having such a framework can ensure that your actions cover the whole range of issues, rather than just focussing on one issue and missing the others. It can also help to put your cyber actions into context, and break down a broad issue into manageable chunks.

### ACTION 2: CYBER FRAMEWORK

Adopt a cyber framework, either similar to the above or something of your own that you are comfortable with.

### CASE STUDY

Scheme A was a relatively large scheme sponsored by a multinational business with a substantial operation in the UK. The pension scheme was administered by a third party, with an in-house pensions function providing trustee executive and secretarial services, including managing all advisers and instructing managers.

Having addressed GDPR in some detail, and having looked at asset transactions, the scheme considered itself well protected against cyber risk – until the sponsor was the subject of a cyber attack, and the in-house pensions team found itself without any systems.

Practical impacts included loss of access to most electronic records and to corporate email systems, inability to instruct advisers (who were reluctant to take instructions from unauthorised sources), no ability to receive sensitive information (personal email accounts were being used but nobody was comfortable with anything other than basic information being shared in that way), and shortage of hardware while corporate hardware was unavailable.

This was compounded by the fact that the pensions team was not a priority in the corporate incident response plan, with the end result being that the in-house pensions team was largely out of action for three to four weeks.
Fortunately, there were no critical projects taking place at the time and there was no lasting damage, but there was substantial disruption and concern. The event highlighted that this was a risk that hadn't really been considered, so there was no plan in place to reduce the risk or recover from it.

# 3. ASSESS - UNDERSTANDING SCHEME VULNERABILITY

## UNDERSTANDING YOUR VULNERABILITY

### BEFORE SCHEMES CAN TAKE STEPS TO PROTECT THEMSELVES AGAINST CYBERCRIME, THEY NEED TO UNDERSTAND WHAT MAKES THEM VULNERABLE.

Research undertaken by Crowe and the University of Portsmouth's Centre for Cybercrime and Fraud Studies (Europe's premier research centre in this area) has considered what makes organisations vulnerable to cybercrime.

The research showed that there are three key factors:

#### 1. HOW ATTRACTIVE IS AN ORGANISATION TO CYBERCRIMINALS?

There are several considerations which can make an organisation attractive to cybercriminals. These include:

- Does the organisation concerned control a lot of detailed personal and financial data which can be used to defraud victims?
- How crucial is the continuity of the function undertaken by the organisation? If a ransomware attack took place which encrypted relevant data, what pressure would there be to pay the ransom demanded?
- Does it control a lot of sensitive data which can be used to threaten and extract ransom payments?
- Does it have high-value intellectual property which can be stolen and sold?
- Is it a potential gateway to mount attacks on other victim organisations (e.g. an outsourced technology provider)?
- Is it known to have weak defences?
- Is it known that it has strong defences and therefore represents a challenge?

The first and second elements are especially relevant to pension schemes and their third-party suppliers. Rich seams of personal and financial data accumulated over decades are a tempting target; also cybercriminals know that the importance of the continuing payment of pensions would mean that, were a ransomware attack to take place, there would be very significant pressure to pay the ransom demanded.

The reason that this 'attractiveness' factor is important is because the 'businesses' who undertake cybercrime, like legitimate businesses, want to attack organisations where the least resource will be needed and the greatest financial gain will be made. Some cybercrime vulnerabilities are visible from the outside with no access to the systems of the organisation concerned, and cybercriminals are now starting to use artificial intelligence to help them select which organisations they attack.

#### 2. WHAT DAMAGE WOULD BE DONE IF AN ATTACK TOOK PLACE?

This is the second factor. The key elements here are:

- Does the organisation concerned have a strong, trusted public profile (and therefore is particularly vulnerable to reputational damage)?
- If its information and data was stolen, could it be used to attack other organisations or individuals?
- Are its income sources vulnerable?
- Is financial damage likely?

The first two elements here are highly relevant to pension schemes and their third-party suppliers. Pension schemes have a high level of public trust, and there is therefore considerable potential for reputational damage. Also, the extensive personal and financial data which they control and process could easily, in the wrong hands, be used to attack beneficiaries.

### 3. HOW CYBERCRIME-RESILIENT IS AN ORGANISATION (AND ITS SUPPLIERS)?

Cyber resilience is not just cyber security. TPR is clear that it is a question of when an attack takes place, not if. There is no technological 'magic bullet' which can protect against all attacks; in part that is because the threat evolves and changes so quickly. To be cyber-resilient an organisation needs three things:

- To be as well protected as possible,
- To be able to manage an attack when/if one happens,
- To be able to recover and mitigate any damage.

This the third key factor which can protect even if an organisation is attractive to cybercriminals and significant damage would occur if an attack was successful.

The National Cyber Security Centre (part of GCHQ) is the lead government organisation dealing with cybercrime. It has a Cyber Assessment Framework (CAF) which cites 14 different factors covering the following four areas:

1. Governance and risk management
2. Protection, awareness and training
3. Event discovery and response
4. Response, recovery and learning lessons.

Pension schemes need to know the extent to which they, their third-party suppliers, and the data flows between them are secure. These assessments provide pension schemes with the information they need to understand their vulnerabilities.

However, this is not a 'one-off' assessment. Because of the rapidly evolving nature of cybercrime, pension schemes need a cyber resilience policy which defines the cyber-resilience expectations they have of all the organisations in their ecosystem, and which sets out how (and how often) compliance will be assessed and the metrics that will be used for the purpose.

This is what 'understanding scheme vulnerability' means.

### ACTION 3: UNDERSTAND VULNERABILITIES

Pension schemes should understand their own vulnerabilities. They should arrange for cyber resilience assessments of themselves, their third-party suppliers and the data flows between them; and should then formulate a cyber resilience policy to ensure that this assessment continues on an ongoing basis and at a frequency commensurate with the rapidly evolving nature of cybercrime.

**Understanding vulnerability – common mistakes to avoid**

1. Don't just look at one part of the pension scheme's ecosystem – it could be attacked at any point, including data in transmission and data already held by third-party suppliers.
2. Trustees have a crucial governance role which can't be delegated to those responsible for the technology.
3. Don't assume where there is a sponsoring employer that they will have done everything that they should – trustees need to find out for themselves.
4. Cybercrime is not just a legal issue to do with GDPR – a ransomware attack does not necessarily involve data loss, and the issues about paying (or not paying) a ransom are complex.
5. Cybercrime is also not just a technology issue – there is no technological 'magic bullet' to ensure everything will stay OK.

Cybercrime is a governance issue like any other important issue for pension schemes, and trustees need to exercise their governance responsibilities after receiving specialist advice provided in plain English.

## ACTION 4: TRAINING

Ensure that trustees, as well as any in-house pensions team, are trained from time to time on the nature of cybercrime, what it is and what it isn't, and how it could impact on the scheme, the members and the sponsor.

# 4. PROTECT – REDUCING YOUR SCHEME'S VULNERABILITY

## WITH RISKS IDENTIFIED, A SCHEME SHOULD ACT TO REDUCE THE LIKELIHOOD OF THOSE RISKS OCCURRING, OR THE IMPACT IF THEY DO OCCUR. THE PRECISE ACTIONS WILL DEPEND ON THE CIRCUMSTANCES OF THE SCHEME, BUT HERE WE HAVE HIGHLIGHTED A NUMBER OF COMMON AREAS:

### MAPPING YOUR CRITICAL ASSETS AND INFORMATION FLOWS

The nature of pension scheme operations is that information flows between a wide number of parties, with all important functions outsourced. Understanding that flow of information is key to assessing and managing cyber risk.

Many schemes started on this journey in 2016, by producing a data map as part of their GDPR compliance. But while that was a good start, for most schemes it was a relatively basic piece of work; it didn't extend beyond membership data, and in many cases it hasn't been looked at since 2016.

More robust mapping of critical assets should be broader than this, both in scope and in detail:

- **Scope** – Why limit the assessment to membership data? Many schemes now have asset maps which document the flow of money around the pensions environment, from company contributions, through investment and disinvestments, to invoices and member payments. Flow of investment instructions is just as important, since if a criminal intercepts your investment instructions they are halfway to intercepting your assets. But why stop there? What other important information flows around the scheme? Covenant information might, for example.
- **Detail** – Understanding that data moves between two parties is helpful, but in itself it is not sufficient to really understand and manage risk. How much data typically moves around? Is it the whole scheme's data, or just individual member data? Is it anonymous or recognisable, and perhaps personally sensitive data? How often does this data get sent? What security is already in place? And is it used reliably?

A more robust approach to data and assets mapping can ensure that schemes focus their questions and actions on the highest-priority areas. It can also ensure that there are no blind spots, where information is being transferred but the trustees don't realise.

### ACTION 5: DATA AND ASSET MAPPING

Arrange for flows of data, assets and other critical information to be mapped, so that the trustees understand the exposure that they have. This will identify areas where attention needs to be focussed, and allow the most effective use of your budget.

### SPONSOR SUPPORT

A common response to cyber risk from pension scheme trustees is: 'The company deals with cyber issues'. In some cases that is true, but in many cases it isn't. It's also necessary to unpack that statement to understand in which areas the company sponsoring the pension scheme might provide support.

Many sponsors do have expertise in cyber risk within their business, although it's worth noting that this can be at very different levels depending on the sponsor and the industry. But the key challenge for pension schemes is often not whether such expertise exists, but whether they can get access to it.

In theory a sponsor may be able to provide support in a range of areas. For example:

- Support with trustee training on cyber risk, and understanding the threat
- Adapting corporate hygiene standards to trustees, possibly including use of company email addresses or technology
- Assessment of third-party providers (piggybacking on the approach the company has to assessing its own suppliers)
- Incident response planning (the company will have its own plan)
- Incident response support (will the company team help to run any incident you have?)
- Legal support on cyber clauses in contracts
- Access to cyber insurance through a corporate policy.

Not all schemes will have access to this support, and even when they do it can be the case that the nature of the support is such that the scheme feels it needs its own approach anyway. For example, a company incident response plan may be so different to what the trustees need that they are better starting from scratch, and although company resources may have deep expertise in cyber issues, most will have no understanding of pensions issues.

The first step is to assess what you have. This will impact on many of the other actions in this guide.

## ACTION 6: SPONSOR SUPPORT

Understand what role the sponsor does and doesn't have when it comes to supporting the scheme on cyber risk. This could relate to training or supporting trustees, assessment of providers, support with contracts or insurance, or dealing with an incident. The level of support you have will influence many of your other actions.

### TRUSTEES

Although most activities of a pension scheme are outsourced, the trustee board is at the centre of most activity, and that role comes with risks that need to be managed. Common issues considered by trustees include:

- Managing trustee email accounts, either by insisting on use of corporate accounts, a dedicated trustee email, or use of a trustee domain. Use of personal email accounts that are used for other purposes is increasingly unusual.
- Mandatory use of a secure portal for sharing information with one another and providers, including meeting packs and exchanges relating to member discretions.
- Regular training to ensure that trustees understand the role that they play in ensuring the scheme is resilient to cyber attacks, on issues such as phishing, two-factor authentication, use of VPNs etc.

Based on Aon's cyber scorecard analysis, around one in three schemes now capture their expectations of trustees in a trustee 'cyber hygiene' document, which trustees can review and confirm that they comply with on a periodic basis. For new trustees this provides a quick and easy introduction to what the board expects from them in relation to cyber security.

## ACTION 7: CYBER HYGIENE

Set out clear expectations for your trustees in relation to cyber security. Capture those expectations in a 'cyber hygiene' document which you can share with existing and new trustees. Your document should be reviewed from time to time to ensure it remains suitable, and compliance with the standards should be checked.

### CASE STUDY

Scheme B had an arrangement where scheme invoices were paid by the sponsor. They found themselves subject to a cyber incident and scam when the chair's email account was compromised.

The trustee chair's email account was compromised as a result of a phishing email, but he didn't realise. The hacker spent time reviewing his email history and contacts, and sent an email to the finance team advising that one of the scheme's major suppliers had changed its bank details. Attached to that was a fake email from the supplier with the new details.

The finance team advised that an email was not sufficient and that a letter would be required. That response was intercepted by the hacker, who replied soon afterwards with a PDF of a letter from the provider, on its headed paper and signed by genuine contacts (all details available from the trustee's email account). The finance team approved the changes and paid a six-figure sum to the fake account.

### PROVIDERS

With most pension scheme activity outsourced, your providers are your first line of defence – and it's increasingly expected that trustees should understand the cyber resilience of those providers.

TPR's April 2018 Guidance states: 'You should assure yourselves that all third-party suppliers have put sufficient controls in place'. The new Single Code states that schemes should 'Assess, at appropriate intervals…the vulnerability of service providers involved in the running of the scheme'.

In making such assessments trustees face a number of questions:

- How often to do such assessments?
- How much detail to go into?
- How much reliance to place on external standards such as Cyber Essentials and ISO27001?
- How to interpret the assessments given that they are not experts?

Although there is still no unified approach being taken by all schemes, some common practices are emerging which we believe are helpful:

- **Frequency** – Schemes should focus on higher-risk providers first, and more frequently, with lower-risk providers subject to less frequent reviews. For example, based on Aon's cyber scorecard over 90% of schemes have done some sort of cyber assessment of their administrator, whereas for other types of provider it is consistently under 50%. The data and asset maps referred to in Chapter 3 can be helpful in ensuring that schemes understand which providers represent the greatest risk.

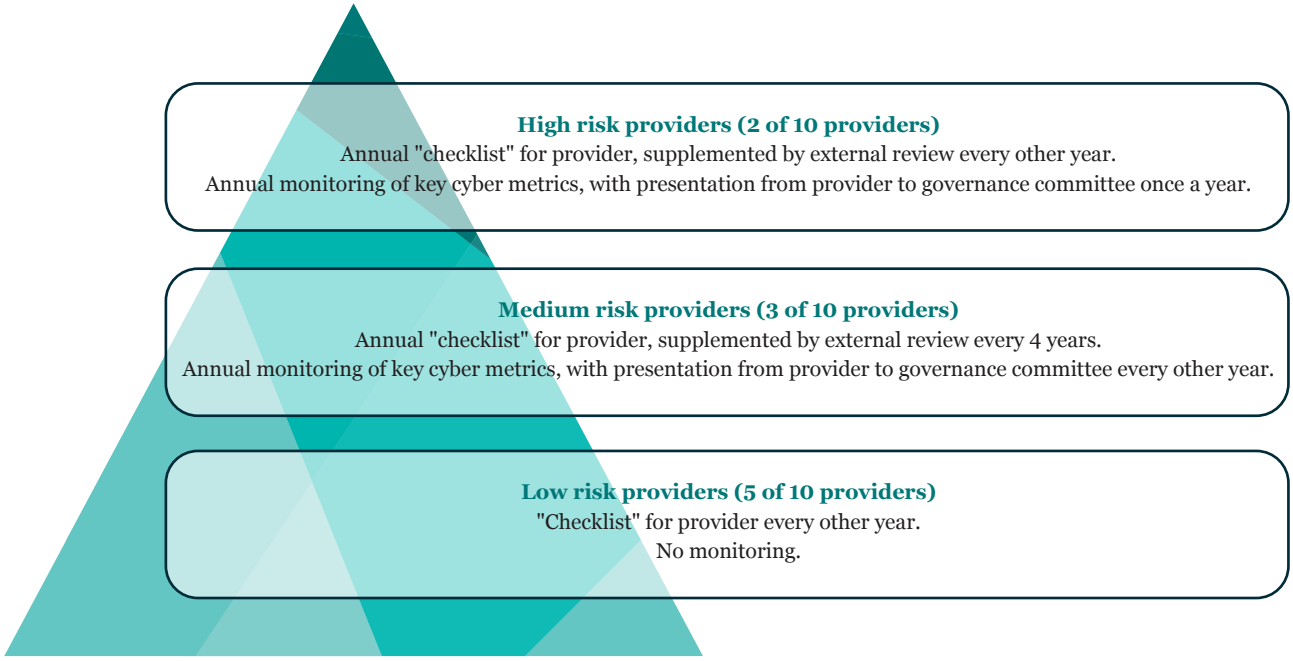
- **Detail** – The type of assessment should also vary based on risk, and approaches are still changing. Early cyber assessments tended to be quite basic and simply ask providers for their cyber policies. Trustees found many of those responses hard to interpret. For large schemes it's now relatively common to ask a third party to assess the cyber resilience of its major providers, but many schemes are also finding that they have expertise within their sponsor, and can piggyback on the approach that the sponsor takes to its own outsourced providers. For some providers reliance on external standards such as ISO27001 may be sufficient, but for other providers trustees may want more detail.
- **In-house teams** – Internal functions, whether administration or a trustee executive/secretarial team, are a particular challenge, and it remains the case that with most in-house teams the reassurances about cyber resilience are being given by the same team that designed and implemented the security. This 'marking your own homework' approach is an area we expect to be more closely scrutinised as the Single Code comes into force.
- **Investment managers** – It is increasingly common for investment consultants to include a cyber assessment as part of their due diligence before putting managers on their 'buy list'. If your manager selection includes that type of review, at outset and on an ongoing basis, then this may be an area on which you do not need to spend much time.
- **Scheme size** – It is clearly the case that larger schemes undertake assessments more frequently and in more detail than smaller schemes, recognising the level of risk and the budgets that they have. This is recognised by TPR, and the April 2018 Guidance specifically states that 'good practice…can be adopted proportionately to the profile of your scheme'.
- **Monitoring** – An area of emerging practice that we are seeing is how to monitor your providers in between formal reviews.

Taking all of this into account, we recommend some practical steps:

- Divide your suppliers into bands, typically high, medium and low risk, recognising that not all providers present the same risk.
- For each band, determine the type and frequency of cyber review and ongoing monitoring that you believe is appropriate, including who will manage that process.
- Document the decisions in a schedule of reviews, which can be part of your cyber policy (see Chapter 6), and be clear who is responsible for managing this.
- Review it from time to time, recognising that this is a developing area, so your needs may change based on your experience of undertaking such reviews.

An example of such an approach is shown in the diagram below.

### Sample hierarchy of provider reviews




A problem faced by many trustee boards is how to understand the results of such assessments, both in an absolute sense (what do the responses mean?) and relative to what should be expected (is the response 'good' or not?). Access to cyber experts, whether from the business or a third party, is essential unless you have genuine cyber expertise on your trustee board. Understanding the assessments also enables trustees to understand which issues need to be followed up, and what they should be asking for.

## ACTION 8: ASSESS PROVIDERS

Divide your providers into risk bands, agree an approach for assessment and ongoing monitoring for each band, and document that in an assessment policy with clear ownership. Ensure you have the expertise to understand the assessments. Follow up on any issues emerging from the reviews.

### CONNECTIONS

While the cyber resilience of your providers and trustees is key, a potential weakness is the connections between them. Every time that data, assets or investment instructions move between two parties there is a risk of that information being intercepted.

The data and asset maps outlined in Chapter 4 provide basic information on those connections. Within this 'protect' stage, the actions are aimed at ensuring that the connections are secure.

As with providers, not all connections present equal risk. A transfer of data that includes sensitive personal data for all members of the scheme is clearly higher risk than a transfer of anonymous data for one member. That said, a simple policy such as 'all data transfers must comply with our agreed security standards' avoids the risk of confusion.

Security around data transfers is now a standard part of operations for most pension scheme advisers, and normally responsibility is taken by the 'sending' party, whether that concerns the anonymisation of data, the password protection, or the use of a secure portal. However, trustees should always check that such controls do indeed exist.

The biggest gap that we see within pension schemes is a lack of security around the movement of investment instructions. While the transfer of assets themselves is generally very secure, around one in three schemes still send investment instructions between trustees and advisers using unencrypted emails. If a cyber criminal can intercept your investment instructions, they are halfway to intercepting your asset movements.

## ACTION 9: CONNECTION PROTECTIONS

Having understood the flows of data, assets and investment instructions between your providers, take steps to improve any perceived weaknesses.

### PROTECTIONS – CONTRACTS AND INSURANCE

The steps so far in this chapter have been about reducing the likelihood or potential impact of a cyber incident. This section is about managing the financial impact of such risks.

The position for pension schemes is complicated, and in some ways more complex than for a large corporate. For any financial loss resulting from a cyber incident, trustees may need to consider:

- **Contracts** – What do provider contracts say about cyber risk, whether it is the cost of dealing with incidents or making good losses?
- **Pension trustee liability insurance** – Are the trustees covered in the event of a cyber incident, and in what circumstances?
- **Corporate cyber insurance** – Is the pension scheme covered under any policy that the sponsor might hold?
- **Trustee cyber insurance** – Does such a policy exist, and in what circumstances can it be called upon?

Trustees will need to take their own advice to properly understand these areas, but a simple guide to each of them is set out below.

#### Contracts

Many schemes have relationships with their advisers which go back for decades, and their contracts may not make any reference to cyber protections or incidents. Even with newer contracts, agreeing cyber terms isn't straightforward.

While providers recognise that they have responsibilities in relation to cyber risk, no provider will provide an open-ended indemnification against the impact of potential cyber attack, and it will be a matter for the scheme and provider to negotiate something appropriate. Providers are also reluctant to commit to specific cyber security arrangements in contracts, as their approaches will change over time to keep up to date with the changing cyber environment. It is reasonable, nevertheless, to expect providers to commit to regular reporting on the issue, and to respond to reasonable queries about their cyber security arrangements.

### Pension trustee liability insurance

In general, pension trustee liability (PTL) insurance does not cover losses arising directly from cyber events. However, if that incident results in a claim against the trustee then the PTL insurance would normally cover the claim. For example, if an incident results in a loss of member data and the trustees incurred costs for legal advice, IT support and communications advice, then that would not be covered. If a member impacted by the event attempted to sue the trustee for negligence in relation to the cyber incident, then the costs related to that claim probably would be covered.

As an alternative to PTL insurance, some trustees have cover through a corporate directors' and officers' (D&O) policy. Similar considerations apply here, but trustees should be aware that some policies exclude cover for acts in the management or administration of pension schemes. If there is no such exclusion, there would be some overlap with what a PTL policy would cover.

### Corporate cyber insurance

Based on Aon's cyber scorecard, around 20% of schemes believe they are covered under a corporate cyber insurance contract. Our experience is that a much lower proportion of schemes have meaningful cover through such a facility. Two issues in particular are worth schemes exploring:

1. Does the policy explicitly cover the scheme? Most policies will not refer to corporate pension schemes; some may refer to 'related entities supported by the sponsor' or similar, but even then the structure of UK schemes may mean they are not covered. Many companies are also reluctant to share policy documents, making it hard to get a definitive answer.
2. Even if the scheme is covered, what type of event is covered, and what level of claim? For example, it would be common for a large multinational to have a policy excess of £10 million or more on a cyber policy, based on its global needs, meaning that any incident impacting the pension scheme is unlikely to be covered.

#### CASE STUDY

Scheme C was advised on a regular basis by the sponsor that the pension scheme was covered under the corporate cyber policy.

Over the course of a few months the scheme obtained access to policy wording which explained that the policy covered 'not-for-profit entities exclusively sponsored by the company or a subsidiary', and arranged confirmation from the insurer that this included the UK pension scheme. The scheme liaised with the insurance team to understand the types of incidents that would and would not be covered.

At the end of the process the insurance team advised that, as the policy had been designed to be appropriate at an overall business level, the excess on the policy was US$25 million per claim. This effectively made the insurance of no use to the scheme, other than in the most exceptional of circumstances.

### Trustee cyber insurance

While there are insurers who have provided cyber insurance for pension schemes in the past, current insurer appetite to provide stand-alone cover is very limited.

A key challenge is that the cyber insurance product is still geared towards corporate buyers, but this is compounded by a general nervousness in the market about cyber risks. Add to that the fact that cyber insurers and underwriters have a very limited knowledge of pension schemes and the risks that they are exposed to, and all of this makes the application and approval process difficult to navigate.

## ACTION 10: CONTRACTS AND INSURANCE

Understand how cyber issues are reflected in contracts with key suppliers. Understand what insurance exists in relation to cyber risks, and agree whether additional cover should be arranged.

# 5. RESPOND – HOW TO DEAL WITH AN INCIDENT

## IT IS IMPORTANT TO BE ABLE TO RESPOND TO A CYBERCRIME INCIDENT. AS DISCUSSED IN CHAPTER 3, THIS IS PART OF CYBER RESILIENCE.

The Guidance from TPR in April 2018 states:

*'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 ensure you understand your third-party suppliers' incident response processes. You should be clear on how and when incidents would be reported to you.'*

### INCIDENT RESPONSE POLICY

There are several points here. First, nobody expects trustees to sit in front of a computer screen as an attack takes place. What is expected is that trustees should exercise their governance responsibilities – in other words, they should have a policy which sets out who will do what and which describes how they will ensure that everyone who has a role does what they are supposed to do.

This should include:

- The roles and responsibilities of the incident response team
- How critical functions and processes can be maintained, and if necessary restored, and the assurances needed from third-party suppliers
- How in-crisis communications will be handled, including how reporting will be made to trustees, beneficiaries and other stakeholders
- The process, thresholds and time limits for notifying other parties, including the ICO and TPR.

Schemes should ensure that they understand their third-party suppliers' incident processes, including how and when they would be informed of a cyber incident at the supplier.

Incidents should be documented, and major incidents should be followed by a post-incident review. Plans should be updated in light of lessons learnt.

The NCSC expands on these points and cites five best-practice elements which those in governance or management positions should ensure are in place. In most organisations, those in such positions will not be directly involved in the technical aspects of a response, but they are responsible for managing the totality of the response and for ensuring that others exercise their responsibilities effectively.

These are:

- **Incident management** – communications, overseeing, tracking and documenting
- **Triage** – understanding the nature, severity and type of incident
- **Escalation**
- **Core response**
- **Post-incident review and closedown** – learning from the incident

In the view of the authors of this guide, 'communications' is so important in this situation that it deserves to be considered separately. Pension schemes need a cyber incident response policy which covers these areas, including how trustees will organise themselves to manage the incident. Training, based on tailored cybercrime scenarios, is then essential to make sure trustees can implement the policy successfully.

We should be clear that this policy is not the kind of *technical* response document which those managing technology for the scheme and its third-party suppliers should have in place. This is a *governance* document.

## ACTION 11: RESPOND EFFECTIVELY

Pension scheme trustees should put in place a cyber incident response policy which allows them to exercise their governance responsibilities effectively, and they should receive scenario-based training on the implementation of this policy.

### SUPPORT DURING YOUR INCIDENT

A key part of your incident response planning is to understand what access the scheme has to specialist expertise should it be required. Most schemes do not have a cyber specialist on their board, or cyber specialists among their advisers.

In practice such support may not be necessary, depending on the nature of the incident. For example, if an incident impacts the scheme administrator then the primary support will be that which the administrator itself needs. However, the scheme may still need specialist support to address areas such as:

- Understanding the issues – there may be information being shared which the trustees don't understand
- Challenge to the provider – are the right questions being asked and are the answers appropriate?
- Practical experience of dealing with a cyber incident, including liaison with the ICO, members and the media.

That support can come from a range of places, but it will most commonly come from the sponsor, a third party or an insurer.

#### Support from the sponsor

Scheme sponsors often have cyber resources, but it can be challenging to access them. More than 60% of schemes completing Aon's cyber scorecard believe they have access to the sponsor's cyber team in the event of an incident; our experience is that the reality is much lower.

Any scheme that believes it has access to corporate support should ask three questions:

- Does the chair of trustees/scheme secretary have the contact name of the person or team that would support the scheme in a cyber incident?
- Does that person know the chair/scheme secretary, and understand enough about the pension scheme to be able to help?
- Is it part of their job description to help the pension scheme in the event of an incident?

If these questions cannot be answered with 'yes', then you still have work to do.

**Support from an insurer**

If you have cover under a cyber insurance contract then part of that cover may be access to specialist support in the event of an incident. Once you call the insurer it is in their interests as much as yours to ensure that an incident is managed.

**Support from a specialist**

The third option that schemes have is to arrange their own specialist support. While this can be arranged at the time, the first action you want to take during a cyber incident probably isn't to start a tender exercise for a cyber adviser. Some schemes, particularly large ones, now have retainers in place with organisations who can help them should an incident take place.

## ACTION 12: INCIDENT RESPONSE SUPPORT

Establish what support you might need in the event of a cyber incident, and ensure that you understand where it would come from. If you are reliant on the sponsor to support you, ensure that is checked in advance.

# 6. GOVERNANCE – DOCUMENTATION AND MONITORING

## CHAPTERS 3 TO 5 PROVIDE A SERIES OF RECOMMENDATIONS WHICH, TOGETHER, WILL MAKE A MATERIAL DIFFERENCE TO THE CYBER RESILIENCE OF A PENSION SCHEME. HAVING ASSESSED THE RISK, PROTECTED THE SCHEME AGAINST IT, AND DEVELOPED PLANS TO RESPOND, THE TASK OF RISK MANAGEMENT IS LARGELY DONE.

In this final chapter we recommend looking at two final points: how you document that strategy, and how you know whether it remains fit for purpose.

### DOCUMENTING YOUR CYBER STRATEGY

In the long term there is no reason that cyber risk should be documented any differently to other risks that schemes have. Schemes have risk registers, integrated risk management frameworks, annual business plans and other documents to ensure that their risks are identified and managed. With the advent of the Single Code we expect to add new concepts such as an 'effective system of governance' and an 'own risk assessment'.

In the short term, however, many schemes are adopting specific cyber policies, or strategies, designed to capture their actions in this area.

The reasons for this are varied, but essentially they are due to the fact that the issue is a relatively new one for trustees. While cyber risk may be integrated with other risks in due course, in the short term a specific cyber policy has a number of advantages:

- It provides a focus to ensure that the issue receives attention.
- It provides a framework to ensure that the issue is looked at holistically.
- It allows responsibilities to be allocated clearly.
- It captures all cyber actions in one place.
- It makes it easy for the trustees to demonstrate to third parties (the sponsor, members or Regulator) that they are taking this seriously and have a plan in place.
- It allows the strategy to evolve and settle before being moved into 'business as usual'.

In documenting your strategy, a question that some trustees ask is 'Can we demonstrate that the actions we are taking meet the requirements placed upon us?'. Whether they are from TPR's April 2018 Guidance, the Master Trust Code or the new Single Code, a cyber policy should allow you to cross-reference your actions with the relevant regulatory requirements, and confirm that for every regulatory requirement you can point to the action you are taking which satisfies that need.

### ACTION 13: DOCUMENTATION

Document your cyber strategy, initially independently of your other risks, until it has matured and can be integrated into your other risk management documents and procedures.

## STAYING RELEVANT

One of the concepts introduced in the new Single Code is the 'own risk assessment'. Despite the name, the own risk assessment is not an assessment of risk – it is an assessment of the risk management process. It asks the question, 'Is our risk management process appropriate and working properly?'.

For cyber risk this is a crucial question, as the risk that schemes are exposed to continues to change, and the expectations in the market of how trustees deal with that risk also continue to change.

Schemes will do this in different ways, but some suggestions based on what we see elsewhere include:

- **Testing your plans** – The IRP testing mentioned in Chapter 5 (Action 11) can highlight gaps in your approach, which then leads to improvements being made.
- **Training from specialists** – None of us have a monopoly on good ideas, and circumstances change: hearing from different specialists will give new insights. This could include independent cyber specialists, or the cyber teams from your advisers or sponsor.
- **Peer group activity** – A common question is 'What is everyone else doing?'; assessments such as the PLSA/Aon cyber scorecard allow you to compare yourself to the market. You can complete this for free at **ww.plsa.co.uk/cyberscorecard**.

However you do this, taking a step back from time to time and checking what you have in place is important. However it's also worth noting that this doesn't mean just keep adding new actions. It's equally relevant to remove actions if they aren't necessary, so that your plans remain focussed and proportionate.

Finally, it's also necessary to ensure that your strategy reflects the latest regulatory requirements. With the new Single Code being implemented this year we hope there won't be new requirements for some time, but inevitably requirements will change at some point.

### ACTION 14: REVIEW PROCESS

Ensure that your overall approach is reviewed and challenged from time to time, to ensure it remains relevant, in line with regulatory requirements and good practice, and that it works. You can compare yourself against other pension schemes at **www.plsa.co.uk/cyberscorecard**.

### ACTION 15: TESTING

Test your incident-readiness on a periodic basis, to ensure that it remains suitable and is broadly familiar to the key people (trustees, pensions team, sponsor). This can be done using scenario-based training, such as a cyber incident simulation.

# 7. THE FUTURE OF CYBERCRIME

## IT IS DIFFICULT TO PREDICT THE FUTURE OF CYBERCRIME, WHICH EVOLVES AND MUTATES AT A FRIGHTENING SPEED. HOWEVER, THERE ARE SOME CHANGES WHICH ARE ALREADY HAPPENING:

- **Artificial intelligence** (AI) and machine learning are already being deployed to increase the automation, speed, frequency and efficiency of attacks, as well as the potential for tailored attacks targeting specific groups. There's also scope to use AI to identify fresh vulnerabilities in networks, devices and applications as they emerge. By rapidly identifying opportunities for human hackers, the job of keeping information secure is made much tougher.
- **The cybercrime-as-a-service** (CaaS) market has also matured over the past few years. What began as a few lone rogue hackers selling user credentials in chatrooms or darknet forums has now evolved into cybercriminals offering a 'menu' of services to those who might be interested in having an attack mounted.

It is also likely that a number of other developments will occur:

- The implementation of highly distributed denial of service attacks using cloud processing, designed to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the internet
- The development of a mature illicit market for virtual items, both stolen and counterfeit
- Physical attacks against data centres and internet exchanges
- Electronic attacks on critical infrastructure, including power supply, transport and data services (the May 2021 attack on the Colonial Pipeline, which carries about 45% of all fuel consumed on the east coast of the United States, is an example of this)
- The growth of cybercrime businesses focussing on high-volume, low-value payments
- Attacks designed to steal biometric information
- Virtual cyber gang wars (as the cybercrime market matures and the room for the growth of these businesses becomes more constricted, it is likely that conflict will increase)
- Advanced criminal intelligence-gathering, including exploitation of big and intelligent data
- High-impact, targeted identity theft and avatar hijacking
- Sophisticated reputation manipulation
- Interference with, and criminal misuse of, unmanned vehicles and robotic devices
- Hacks against connected devices with direct physical impact (car-to-car communications, heads-up display and other wearable technology, etc.).

It should not be doubted that these changes will affect pension schemes and their third-party suppliers. In this context it is difficult to see law enforcement having much impact on attacks once they have happened, but, more positively, the NCSC should continue to do a good job developing awareness, setting standards and encouraging better protection. TPR has also substantially developed its focus in this area with new guidance in the Single Joint Code.

The prospect of increasingly sophisticated cybercrime is not one which helps any of us to sleep better at night, and it should impel every pension scheme to get properly protected. However, it would be wrong not to reflect on some of the more positive trends which may extend into the future.

There is a growing understanding among pension schemes that cybercrime is not like other static risks which appear on risk registers alongside mitigating controls. It evolves and develops more like a clinical virus, and cybercrime protection measures need to be equally dynamic.

Also, more and more schemes are understanding that this is not just a technology problem – there is no technological 'magic bullet' which can provide 100% protection. It is a question of when an attack happens not if, and it is a governance issue. How and with what metrics will those in governance positions understand and manage levels of cybercrime protection and respond when an attack occurs? That is the key question for the future.

This understanding needs to continue to develop, and at a speed commensurate with the evolution of the problem, so that the challenge of staying properly protected is met. It is hoped that this guide (and regular future updates) will play its part.

# APPENDIX 1
# ACTIONS CHECKLIST

The actions from the guide are summarised below.

**ACTION 1: SPECIALIST SKILLS**
Trustees should review whether they have access to genuinely specialist advice concerning how to properly protect their pension schemes.

**ACTION 2: CYBER FRAMEWORK**
Adopt a cyber framework, either similar to the above or something of your own that you are comfortable with.

**ACTION 3: UNDERSTAND VULNERABILITIES**
Pension schemes should understand their own vulnerabilities. They should arrange for cyber resilience assessments of themselves, their third-party suppliers and the data flows between them, and should formulate a cyber resilience policy to ensure that this assessment continues on an ongoing basis and at a frequency commensurate with the rapidly evolving nature of cybercrime.

**ACTION 4: TRAINING**
Ensure that trustees, as well as any in-house pensions team, are trained from time to time on the nature of cybercrime risk, what it is and what it isn't, and how it could impact on the scheme, the members and the sponsor.

**ACTION 5: DATA AND ASSET MAPPING**
Arrange for flows of data, assets and other critical information to be mapped, so that the trustees understand the exposure that they have. This will identify areas where attention needs to be focussed, and allow most effective spend of your budget.

**ACTION 6: SPONSOR SUPPORT**
Understand what roles the sponsor does and doesn't have when it comes to supporting the scheme on cyber risk. This could relate to training or supporting trustees, assessment of providers, support with contracts or insurance, or dealing with an incident. The level of support you have will influence many of your other actions.

**ACTION 7: CYBER HYGIENE**
Set out clear expectations for your trustees in relation to cyber security. Capture those expectations in a cyber-hygiene document which you can share with existing and new trustees. Your document should be reviewed from time to time to ensure it remains suitable, and compliance with the standards should be checked.

**ACTION 8: ASSESS PROVIDERS**
Divide your providers into risk bands, agree an approach for assessment and ongoing monitoring for each band, and document that in an assessment policy with clear ownership. Ensure you have the expertise to understand the assessments. Follow up on any issues emerging from the reviews.

**ACTION 9: CONNECTION PROTECTIONS**
Having understood the flows of data, assets and investment instructions between your providers, take steps to improve any perceived weaknesses.

**ACTION 10: CONTRACTS AND INSURANCE**
Understand how cyber issues are reflected in contracts with key suppliers. Understand what insurance exists in relation to cyber risks, and agree whether additional cover should be arranged.

**ACTION 11: RESPOND EFFECTIVELY**
Pension schemes should put in place a cyber incident response policy which allows them to exercise their governance responsibilities effectively, and should receive scenario-based training on the implementation of this policy.

**ACTION 12: INCIDENT RESPONSE SUPPORT**
Establish what support you might need in the event of a cyber incident, and ensure that you understand where it would come from. If you are reliant on the sponsor to support you, ensure this is checked in advance.

**ACTION 13: DOCUMENTATION**
Document your cyber strategy, initially independently of your other risks, until it has matured and can be integrated into your other risk management documents and procedures.

**ACTION 14: REVIEW PROCESS**
Ensure that your overall approach is reviewed and challenged from time to time, to ensure it remains relevant, in line with regulatory requirements and good practice, and that it works.

**ACTION 15: TESTING**
Test your incident-readiness on a periodic basis, to ensure that it remains suitable and is broadly familiar to the key people (trustees, pensions team, sponsor). This can be done using scenario-based training such as a cyber incident simulation.

# APPENDIX 2 WHERE TO GET MORE INFORMATION

The following sources (not comprehensive, and ever-evolving) provide useful guidance and additional information:

- **The Pensions Regulator** – Cyber guidance for pension schemes
  https://www.thepensionsregulator.gov.uk/-/media/thepensionsregulator/files/import/pdf/cyber-security-principles-for-trustees.ashx
- **PRAG Cybercrime protection guidance** – https://www.prag.org.uk/
- **PASA Cybercrime protection guidance** – https://www.pasa-uk.com/cybercrime-and-fraud/
- **Information Commissioner's Office (ICO)**:
  https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf
- **National Cyber Security Centre (NCSC)**:
  https://www.ncsc.gov.uk/cyberessentials/overview
  https://www.ncsc.gov.uk/section/advice-guidance/all-topics
- **ICO** and **NCSC**:
  https://ico.org.uk/for-organisations/security-outcomes/
- **FCA**:
  https://www.handbook.fca.org.uk/handbook/FCG/5/?view=chapter
  https://www.fca.org.uk/publications/research/cyber-security-industry-insights
  https://www.fca.org.uk/publication/research/technology-cyber-resilience-questionnaire-cross-sector-report.pdf
  https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf
- There are two relevant ISO Standards:
  **ISO27001** – https://www.iso.org/isoiec-27001-information-security.html
  **ISO27032** – https://www.iso.org/standard/44375.html
- **City of London Police** – Cyber Griffin
  https://cybergriffin.police.uk/
- Crowe and Aon's sites also contain useful advice and comment:
  **Aon** – https://www.aon.com/unitedkingdom/retirement-investment/trustee-effectiveness/cyber-threats-to-corporate-pension-schemes.jsp
  **Crowe** – https://www.crowe.com/uk/croweuk/services/advisory/forensic-services
- **PLSA** – The PLSA/Aon cyber scorecard
  www.plsa.co.uk/cyberscorecard
  www.plsa.co.uk/cyberscorecardlgps

**Pensions and Lifetime Savings Association**
24 Chiswell Street
London EC1Y 4TY

T: 020 7601 1700
E: plsa@plsa.co.uk

**www.plsa.co.uk**

*June 2022*