Cyber Resilience and Business Continuity: A Timely Opportunity for Reassurance

November 2026

Introduction

Recent comments from the Government about the need for organisations to prepare for cyber incidents, supply chain disruption and climate-related emergencies provide a useful moment for pension scheme trustees to reflect on their own resilience arrangements. Speaking as part of a wider national resilience initiative, ministers emphasised that cyber-attacks, technology failures, severe weather events and other disruptive events are likely to become increasingly common features of the operating environment.

For pension schemes, these themes are far from new. Cyber security, business continuity, operational resilience and climate-related risks have featured on trustee agendas for many years, supported by guidance from The Pensions Regulator and a growing focus on the resilience of critical service providers. Nevertheless, recent events offer a useful reminder of why this work matters.

This briefing is intended for professional trustees, pension scheme sponsors, employers and professional advisers. It is not intended for retail clients or individual members and should not be relied upon as personal financial, tax or legal advice.

When Preparation Prevents the Crisis

The recent concerns surrounding the PHP vulnerability attracted considerable attention across government and industry. Given the widespread use of the technology, the potential implications were significant and prompted precautionary action from many organisations.

Yet, for most people, the lasting impression may simply be that very little happened.

That would be the wrong conclusion.

In many respects, the lack of widespread disruption demonstrates why investment in resilience is so important. The response involved significant effort by technology providers, cyber specialists, infrastructure operators and organisations seeking to understand their exposure and implement mitigations. Systems were reviewed, contingency arrangements activated and vulnerabilities addressed before they could lead to wider operational impacts.

There is perhaps a parallel with the Millennium Bug. The fact that major disruption failed to materialise was not evidence that the risk was overstated. Rather, it reflected the success of the extensive preparation undertaken beforehand.

The same principle applies to trustee governance. Effective resilience arrangements are often judged by events that never occur because appropriate planning has reduced the likelihood or impact of disruption.

Understanding the Wider Risk Environment

The Government's recent resilience messaging is also notable because it extends beyond cyber security alone. Alongside increasingly sophisticated cyber threats, ministers have highlighted supply chain disruption, severe weather events and broader infrastructure risks as areas requiring greater preparedness.

This reflects an important reality for pension schemes. Operational disruption does not always originate within the scheme itself, or even within its immediate service providers.

Trustees rely on a complex ecosystem of administrators, insurers, payroll providers, AVC providers, software platforms, cloud infrastructure and professional advisers. Any one of these organisations may in turn depend on technologies, networks and suppliers that are largely invisible to trustee boards.

As a result, resilience is increasingly about understanding dependencies and ensuring there are robust arrangements in place when unexpected events occur. The issue is often less about preventing every possible disruption and more about ensuring key services can continue and recover effectively when disruption does arise.

A Good Time to Seek Reassurance

For most schemes, recent events should not be viewed as a reason to revisit existing strategies fundamentally or introduce entirely new controls.

Many trustee boards already operate within well-developed governance frameworks. Risk registers are maintained, business continuity plans are documented, cyber risks are discussed with key providers and incident response arrangements are in place. That foundation remains important.

However, periods such as this can provide a useful opportunity to seek reassurance. Trustees may wish to revisit assumptions made during previous risk reviews, understand any lessons learned by service providers and confirm that contingency arrangements remain current, practical and accessible.

The objective is not necessarily to identify gaps. In many cases, the conclusion may simply be that existing arrangements continue to provide an appropriate level of protection. Equally, the discussion may highlight opportunities to strengthen trustee understanding of key dependencies or improve documentation and escalation processes.

Suggested Actions for Trustees

Trustees may wish to consider:

- seeking an update from administrators and other key service providers on any lessons learned from recent cyber or operational resilience events;
- reviewing whether business continuity and disaster recovery arrangements remain up to date and appropriately tested;

- considering whether current risk registers adequately reflect cyber, climate-related and supply chain risks;
- reviewing crisis management and member communication arrangements in the event of significant service disruption; and
- exploring whether scenario testing or resilience exercises could provide additional assurance to the trustee board.

Conclusion

The key lesson from recent events is not that trustees should be alarmed. If anything, the PHP episode demonstrated the benefits of preparation, strong governance and effective risk management. The fact that widespread disruption was largely avoided should provide reassurance that resilience planning can make a meaningful difference when risks emerge.

Against a backdrop of increasing technological dependence, evolving cyber threats and growing attention on national resilience, now may simply be a good time for trustees to confirm that the arrangements they already have in place remain capable of protecting the scheme and its members when they are needed most.

Find out more

For more information on how Broadstone can help you, please contact your Broadstone consultant on:



+44 (0) 20 3869 6830
+44 (0) 7976 198 044
david.brooks@broadstone.co.uk

Contact

020 3869 6900

corporate@broadstone.co.uk

broadstone.co.uk

@Broadstone_Ltd

company/thebroadstonegroup

Birmingham / Bristol / Coventry / Darlington / Edinburgh / Glasgow / High Wycombe
London / Manchester / Redditch / Sheffield / St Albans / York

Important Information:

This document is for information purposes only and does not constitute advice or a personal recommendation. It is based on current legislation and HMRC guidance, which may change. Outcomes depend on individual circumstances and should not be assumed. No warranty is given as to accuracy or completeness, and no liability is accepted for reliance on this content. Professional advice should be sought before taking any action.

Broadstone Administration Limited (BAL), Broadstone Corporate Benefits Limited (BCBL), Broadstone Financial Solutions Limited (BFSL) and Broadstone Regulatory & Risk Advisory Limited (BRRAL) are companies registered in England and Wales with Companies House numbers 16262678, 07978187, 02131269 and 04663795 respectively with their registered offices at 100 Wood Street, London EC2V 7AN. BCBL and BFSL are authorised and regulated by the Financial Conduct Authority (Financial Services Register numbers 587699 and 134771 respectively). Each of the above companies use the trading name Broadstone, which is a trademark owned by BCBL and used by companies in the Broadstone group.