Week commencing 23 November 2026

ClearPath Partnership

COVERAGE
9 – 22 November 2026

AUDIENCE
IT and security leadership · compliance and risk leads · programme directors

HANDLING
Internal use — not for onward distribution

IF YOU JUST REMEMBER ONE THING FROM THIS BRIEFING…

A government grant can now fund your subcontractors' Cyber Essentials — but only if you have signed the Cyber Resilience Pledge.

The £9.4m package launched on 3 November funds first-time Cyber Essentials certification for SME suppliers of Cyber Resilience Pledge signatories, worth up to £7m through March 2029. Ask this week: have we signed the Pledge, and have we told our subcontractors the funding exists.

THIS FORTNIGHT

Incidents and sector activity

PRIORITY

9 NOV

CISA adds IBM Aspera Faspex file-transfer flaw to its exploited-vulnerability catalogue

CVE-2026-123218, a maximum-severity (9.8) authorisation-bypass flaw in IBM Aspera Faspex 5.0.0–5.0.19, lets an authenticated user seize full administrative privileges. CISA added it to the KEV catalogue on 9 November with a three-day federal deadline. IBM's fix is Faspex 5.0.19 PL1.

So what: managed file-transfer tools carry drawing packages and contract documents between consultants and contractors. Find any Aspera Faspex instance and patch to 5.0.19 PL1 now; the federal deadline has passed.

WATCH

7-9 NOV

Qilin claims Amber Management & Engineering Services; claim unconfirmed

Ransomware group Qilin listed Amber Management & Engineering Services, a UK building-services engineering consultancy, on its leak site, with an attack dated 7 November and the listing surfacing two days later. Leak size is unspecified and the company has made no statement; treat the claim as unconfirmed.

So what: Qilin's affiliates typically get in through unpatched VPN appliances, missing MFA or exposed management interfaces. If you work with this supplier, check exposure directly rather than waiting for a leak.

WATCH

3 NOV

Government launches £9.4m Cyber Essentials funding package for SME suppliers

DSIT's package has two parts: a £2.4m First Step Fund giving any SME a 75% discount on its first Cyber Essentials certificate, and a Cyber Resilience Pledge supplier grant (up to £7m, to March 2029) that fully funds SME suppliers of Pledge-signatory organisations.

So what: sign the Pledge, or point existing signatories' funding at your own supply chain, before competitors do.

WATCH

ONGOING

Cyber Security and Resilience Bill's Commons return remains unconfirmed

Lords Third Reading was listed for 2 November, after the government's two Report Stage defeats on 26 October. We found no confirmation that Third Reading completed or that the bill has reached the Commons. MLex reported ministers were still under pressure to accept a late scope-review amendment.

So what: if you supply CNI operators or MSPs, the vendor-direction and scope provisions remain unsettled. Do not assume the bill's current drafting is final.

ACTION QUEUE

Changes and vulnerabilities to act on this fortnight

CHANGE OR VULNERABILITY	WHAT IT APPLIES TO	WHY IT MATTERS ON A PROJECT	ACT BY
CVE-2026-123218	IBM Aspera Faspex (file transfer)	Admin-bypass flaw on platforms used to move drawings and contract packages.	Overdue
Cyber Essentials First Step Fund	Any SME, first-time CE applicant	75% discount removes the cost barrier for small subcontractors.	Apply now
Cyber Resilience Pledge supplier grant	SME suppliers of Pledge signatories	Fully funds CE certification across your subcontractor base.	To Mar 2029
CS&R Bill Commons stage	CNI suppliers, MSPs, data centres	Scope and vendor-direction provisions unsettled before return to MPs.	Watch
Cyber Essentials Danzell question set	CE Plus candidates assessed under Willow	Willow closed 27 Oct; Plus candidates must finish under it.	27 Jan 2027

Identifiers as published in the CISA KEV catalogue and gov.uk scheme guidance. Confirm against your own asset inventory before acting.

REGULATORY AND SECTOR WATCH

What changed, and what is coming

In force now

- The £9.4m Cyber Essentials funding package — the First Step Fund and the Resilience Pledge supplier grant — is live, administered through IASME.
- Cyber Essentials Danzell (v3.3) remains the only question set for new assessments.

Approaching

- Cyber Essentials Plus candidates assessed under Willow have until 27 January 2027 to complete under the outgoing question set.
- The CS&R Bill returns to the Commons for consideration of Lords amendments; no confirmed date.

Standing watch — Robert Hitchins Limited. The Majinahanashi leak claim from 12 October remains unconfirmed six weeks on, with no company statement and no published data. Treat leak-site claims as a prompt to check exposure, not as fact.

RECOMMENDED

Three things to do before the next edition

- Locate any IBM Aspera Faspex instance in your estate and patch to 5.0.19 PL1 immediately.
- Check whether your organisation can sign the Cyber Resilience Pledge to fund subcontractor Cyber Essentials certification.
- Confirm any Cyber Essentials Plus assessment still on the Willow question set is finished well before January.

OUTLOOK — NEXT FORTNIGHT

We assess it is likely further managed file-transfer or remote-access products join the KEV catalogue before the next edition. It is a realistic possibility the Resilience Bill completes its Commons stage within the fortnight, and a realistic possibility the Amber Management claim is confirmed or withdrawn.

NEXT EDITION

Monday 7 December 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.

ClearPath Partnership