FOR HEALTHCARE LEADERS
HSJ

The cyber security risk you are (probably) overlooking

By Vsevolod Shabad | 4 December 2025

The new assessment framework strengthens NHS cyber security, but increased recognition of the impact of staff behaviour is vital if the service is to be properly protected

The shift from the Data Security and Protection Toolkit (DSPT) to the Cyber Assessment Framework (CAF) represents an important move towards more honest, evidence-based cyber assurance in the NHS. CAF is a stronger model: it focuses on observable practice rather than documents, and it draws attention to real security control operations rather than the narratives that often grow around it.

But evidence-based assurance also changes organisational behaviour – sometimes in predictable and unhelpful ways – and this aspect receives far too little attention.

Across 40 years working in critical infrastructure sectors in Europe and Asia – including banking, energy and, more recently, telecoms – I have seen the same pattern emerge whenever organisations adopt evidence-driven assurance frameworks. Once indicators become the basis for scrutiny, teams naturally optimise for those indicators rather than for the underlying risk.

Behavioural research shows that under pressure, people default to what is visible and achievable – a mix of present bias, availability bias and anchoring that shapes organisational effort just as much as individual judgement. Not because anyone intends to mislead, but because people work under intense operational pressure, resources are stretched, and visible indicators attract effort more reliably than invisible structural work.

The NHS is no exception. CAF's outcomes and indicators require careful judgement, and trusts begin from very uneven starting positions. Some run modern estates with mature digital teams. Others must manage fragmented legacy infrastru funding gaps. Under these haviour loops tend to appear.

Ask HSJ
COOKIE SETTINGS

Strong and weak are both vulnerable

First, the more digitally mature trusts can encounter a premature assurance “ceiling”. Once the expected CAF evidence for an outcome is provided, the framework struggles to surface the continuing work required simply to hold ground. Yet against today’s threat landscape, staying still is not really an option. Attackers move faster, tools are more widely available, and vulnerabilities are exploited more quickly.

It becomes a cyber version of the Red Queen problem: teams have to keep running just to remain in the same place. On paper, though, their posture can appear static even when the effort required simply to avoid slipping backwards is increasing every month.

Second, the trusts with significant legacy estates face the opposite pressure. When the gap to CAF expectations feels unmanageable, staff naturally concentrate on what is easiest to evidence. The effect is predictable from behavioural economics: people anchor on achievable tasks, narrow their focus to what demonstrates progress, and downplay the deeper risks that are harder to surface. Again, this is not malpractice – it is a rational adaptation to the incentive environment.

> ***CAF is a necessary step forward. But assurance works best when it considers both state and movement. In a landscape where cyber risk rapidly becomes patient risk, clarity about improvement is not a luxury – it is part of the assurance the NHS owes to the public***

These effects become sharper still in the post-2025 landscape. The restructuring of NHS England, including the substantial reduction

Ask HSJ

ams, means the centre has far less

COOKIE SETTINGS

capacity to interpret extensive narrative assurance. A model that depends heavily on qualitative judgement becomes harder to operate just as the system becomes more devolved.

None of this undermines CAF. It remains a necessary and more honest model of assurance than what preceded it. But if we want CAF to work in real operational conditions, we need to recognise the behavioural patterns it can unintentionally drive.

One practical improvement, used in other critical-infrastructure sectors, is to pair state-based assurance with a small set of movement-based signals. These are not new frameworks, and they should not mean more paperwork. Their purpose is simply to show whether the underlying cyber posture is improving, stagnating or quietly slipping backwards.

Even simple illustrative movement indicators – for example, whether long-standing vulnerabilities are reducing, whether key legacy interfaces are being retired at a steady pace, or whether high-risk backlogs are shrinking rather than growing – can reveal truths that static evidence cannot.

These signals are inherently harder to manipulate without doing the underlying work, and they help boards and the public distinguish genuine improvement from cosmetic compliance. They also create fairer visibility across uneven trusts: an organisation with heavy technical debt can still demonstrate strong movement even if its absolute state remains behind its peers.

For a leaner NHSE, progress signals offer an additional advantage: an early-warning mechanism that does not require deep interpretive capacity. In a more devolved environment, they allow the centre to see where risk is trending without reviewing dozens of complex assurance submissions.

The approach is straightforward to test in practice, and experience from other sectors shows that even small pilots can generate rapid learning.

CAF is a necessary step forward. But assurance works best when it considers both state and movement. In a landscape where cyber risk rapidly becomes patient risk, clarity about improvement is not a luxury – it is part of the assurance the NHS owes to the public.

Ask HSJ

COOKIE SETTINGS