FOR HEALTHCARE LEADERS HSJ

Boards must take their responsibility for cyber security more seriously

By Vsevolod Shabad | 21 November 2025

Cyberattacks keep crippling NHS services not due to missing technology, but predictable board-level governance failures that leave known vulnerabilities unaddressed

The Synnovis ransomware attack in June 2024 cancelled 10,000 appointments and forced hospitals to rely on manual blood-test processing for weeks – cost: £32.7m. Seven years earlier, WannaCry paralysed 80 NHS trusts – cost: £92m.

Different attacks. Same governance failure.

This isn't about technology gaps or underfunding. Following WannaCry, investigations revealed that affected trusts had "appropriate governance structures" and "qualified staff". Cybersecurity professionals identified threats, recommended fixes, and had available patches. What failed was decision-making at the board level.

Post-WannaCry, we added regulations, enhanced the data security and protection toolkit (DSPT) requirements, and strengthened oversight. Synnovis proves we're still solving the wrong problem. The issue isn't that boards lack resources or ignore frameworks – it's that frameworks themselves create predictable traps.

The three traps

Trap 1: Anchoring on outdated plans.

Before WannaCry, NHS trusts had documented Windows migration plans from 2014 with five-year timelines. When critical vulnerabilities emerged in March 2017, boards reviewed them against those plans and maintained approved schedules. The documented plan became organisational truth, appearing in strategic documents, budget allocations, and quarterly updates. Each appearance reinforced its validity.

When WannaCry struck 58 days later, migrations were still "on track". Boards had anchored on three-year-old assumptions while threats evolved daily.

This wasn't irrational. Boards weighed certain immediate risks – service disruption from emergency changes – against uncertain future threats. However, this pattern persists: multi-year digital transformation programmes continue unchanged, while national alerts warn of active exploitation.

Trap 2: Overconfidence from compliance metrics.

Boards receive reassuring metrics: DSPT standards are met, assessments are completed, policies are updated, and staff are trained. These create confidence divorced from actual capability.

Before WannaCry, officials cited "88 on-site assessments completed" as evidence of preparedness. What went unmentioned: 63 per cent of trusts remained unassessed, and assessments measured process documentation rather than performance under pressure.

Compliance frameworks ask, "Do procedures exist?" The critical question is "Do procedures work when systems fail?" Most boards don't know because documented plans are rarely tested under realistic conditions.

Before Synnovis, affected organisations likely had documented business continuity plans and disaster recovery procedures. The attack revealed whether those plans actually worked. The gap between "procedures documented" and "procedures effective" can cost tens of millions.

Trap 3: Sunk cost paralysis.

Multi-year programmes accumulate organisational momentum. When emergency threats emerge, boards face uncomfortable trade-offs: abandon initiatives with substantial investment, or maintain timelines and accept risk.

Before WannaCry, the Windows migration had 36 months of invested effort when emergency patching became critical. Boards asking "Should we pause for emergency response?" faced internal resistance: finance teams questioning budget reallocations, project managers defending milestones, and executives concerned about explaining changes to regulators.

Maintaining the approved plan felt safer than justifying deviation, even when circumstances had fundamentally changed. This pattern repeats whenever boards must choose between continuing familiar initiatives and responding to novel threats.

What boards should do?

Breaking these patterns requires concrete action. Quarterly reviews should include a forcing question: "Which documented plans remain valid given current threat intelligence?" When national alerts warn of active exploitation, ask: "Does our current programme of work address these threats, or are we executing last year's plans while today's vulnerabilities remain undefended?"

If the answer requires referencing three-year-old strategy documents, your governance structure likely failed to adapt.

Cyber security plans should be tested under realistic conditions. Start with the National Cyber Security Centre (NCSC) Exercise in a Box – free, board-level scenarios requiring no technical setup. Progress through tabletop exercises testing coordination, then technical penetration testing, revealing actual vulnerabilities.

The NHS already tests operational resilience through emergency preparedness, resilience and response (EPRR) exercises for mass casualties and severe weather. Extending this to cyber resilience means progressive testing – announced drills during quiet periods first, with clinical leadership approval and immediate abort protocols.

Can staff actually execute manual prescribing procedures when the electronic system fails? Most boards assume yes because procedures are documented. Testing reveals whether documentation reflects reality.

The 58-day WannaCry window exceeded normal governance cycles. Boards meet quarterly; committees meet five times yearly. When alerts warn of active exploitation, waiting for scheduled meetings is a structural failure.

Boards should pre-authorise emergency responses based on threat severity. For critical alerts – active exploitation, patient safety impact – delegate authority to the trust's chief information security officer with immediate board notification and formal ratification within seven days. The board maintains oversight without becoming a decision-making bottleneck.

Concurrent cybersecurity initiatives should be capped at a maximum of five. Each quarter, boards must explicitly decide for each initiative: complete, continue with the current justification, or abandon. No initiative remains "in progress" indefinitely without revalidation against the current threat landscape.

This forces trade-offs into the open. When critical vulnerabilities emerge, boards must answer: "What do we stop doing to address this threat?" The question makes sunk costs visible and challengeable.

The window is closing

NHS digital transformation – AI diagnostics, integrated records, remote monitoring – is now entirely dependent on cyber resilience. Yet governance structures built for annual planning cycles cannot manage threats that evolve weekly, or technologies such as AI that shift in capability month by month.

Another major incident is inevitable. Whether it costs £30m or £300m depends on whether boards recognise that governance structures – not IT teams – created the conditions for WannaCry and Synnovis.

NHS boards followed recognised best practice and still enabled Synnovis. That should concern every non-executive director in the system. The steps above are not optional enhancements; they are urgent requirements for safe, modern healthcare.

The evidence is clear. The solutions exist. Whether we act on them now – or repeat the same failures – is a board-level choice.