HIMSS 26
EUROPE
19–21 May | Copenhagen

Joe Harper
Director of ICT

EXPERT **INSIGHTS**
EXCEPTIONAL **IMPACT**

#HIMSS26EUROPE

Cyber Security in a UK NHS Foundation Trust

HIMSS 26

Why this matters

- In the NHS, cyber security is a patient safety and service continuity issue
- Disruption affects clinical decisions, diagnostics, and operational flow
- Threats are evolving faster than replacement cycles and funding
- Our job: reduce harm and shorten recovery time — not chase perfection

About King's

- Large London teaching hospital trust delivering acute and specialist care serving a complex population
- Digitally dependent: EPR, diagnostics, imaging, theatres, and community links
- Multi-site operations: resilience and standardisation is difficult
- A realistic profile for many public hospitals: complex estate + constrained funding

Current situation (UK NHS reality)

- Legacy and modern platforms run side-by-side
- Large attack surface: users, suppliers, endpoints, and connected clinical tech
- Continuous compliance expectations (e.g., DSPT, CAF-aligned assurance)
- Threats like ransomware, phishing, and supply chain attacks continue to pose serious risks to healthcare data security

New cyber challenges in clinical settings

- AI in clinical workflows: governance, validation, and safe use
- Data sovereignty: control, jurisdiction, and assurance under stress
- Medical devices: long lifecycles, patching limits, and operational fragility

Governance decisions boards must make

- Name accountability: SIRO ownership and an executive lead for cyber risk
- Make risk decisions explicit: what is mitigated, accepted, or transferred
- Require assurance: how risks are shown in dashboards and reviewed regularly
- Test readiness: can critical services be maintained during a prolonged incident?

When the budget is constrained

- Prioritise by patient harm: focus on the failures with the biggest clinical impact
- Bias to resilience: reduce blast radius (identity, segmentation, recovery)
- Prefer control families that scale: standards, templates, automation, reuse
- Invest in people and rehearsal: culture + response beats more tooling

Cyber resilience is a leadership responsibility

- Leadership Shapes Cyber Resilience
  - Cyber resilience depends more on leadership intent and decisions than on technical expertise.
- Risk Tolerance and Preparedness
  - Effective cyber resilience requires leaders to define acceptable risk levels and investment in preparedness.
- Clear Communication Builds Trust
  - Transparent communication of cyber risk decisions strengthens trust among clinicians, patients, and regulators.
- Decisive Leadership in Uncertainty
  - Leaders must confidently guide their organisations through cyber threats despite inherent uncertainties.

Advice for boards (what to do next week)

- Ask the right questions: ownership, critical assets, and incident endurance
- Use DSPT evidence to inform board risk discussion and investment choices
- Insist on routine exercising: ‘table-top’ and live recovery validation
- Align cyber risk to patient safety risks in the Board Assurance Framework
  - Reference: NHS England Digital ‘Cyber security guide for executive and non-executive directors – Questions for the board’
  - Reference: Data Security and Protection Toolkit (DSPT) – board assurance baseline

Board checklist

Who owns cyber risk (SIRO/board lead)? •
What are our critical assets? •
How is risk shown/reviewed (dashboards)? •
Have we reviewed DSPT? •
Can we maintain services during an incident?

HIMSS 26
EUROPE

Thank you