HIMSS 26
EUROPE
19–21 May | Copenhagen

From Threat to Action: Insights from Germany's € 1.8bn Cyber Programme

Federal Ministry of Health Germany
Division 512

EXPERT INSIGHTS
EXCEPTIONAL IMPACT

#HIMSS26EUROPE

DISCLAIMER: The views and opinions expressed in this presentation are solely those of the author/presenter and do not necessarily represent any policy or position of HIMSS.

Today's Journey — 20 Minutes

HIMSS26 EUROPE · COPENHAGEN

1

The problem

Where Healthcare Stands Today · 3 min

2

The Next Wave

Five Emerging Threat Vectors · 7 min

3

Policy & Governance

What Regulators Are Demanding · 4 min

4

Strategic Action Plan

From Boardroom to Operations · 4 min

5

Key Takeaways

Three Actions for Monday Morning · 2 min

01 · The challenge

HIMSS 26

#1 The challenge

Why this matters:

Every connected system is a potential attack surface: EHR systems, infusion pumps, imaging scanners, lab automation.

A single ransomware attack can force a hospital into paper-based operations for weeks, cancel surgeries, redirect emergency patients.

This is not an IT problem. It is a patient safety problem.

€1.8 Billion

- Healthcare was the most affected sector in EU NIS incident reporting for four consecutive years 2020-2023 (ENISA/CIRAS).
- 2nd most attacked sector in Germany: 156 healthcare incidents in 2025, +23 % year-on-year (BSI Threat Report 2025).
- The German Federal Ministry of Health launched the "Sofortprogramm Cybersicherheit": EUR 1.8 billion emergency programme 2026-2029, covering up to 4,000 health facilities.

Modern healthcare is fundamentally IT-dependent.Cyberattacks carry the potential to endanger patient safety and human life.

When Systems Fail

2020 · Uniklinik Duesseldorf — Emergency department closed after ransomware. **Patient death** reported.

2022 · Klinik Lippe, Germany — Multiple surgeries cancelled; affiliated MVZ facilities shut down.

2022 · Medical Campus Bodensee — Complete 2-day IT outage; no access to digital patient records.

2023 · Uniklinik Frankfurt — Full network disconnection; weeks of manual paper-based operations.

2024 · AEP Pharma — Unable to deliver medications to hospitals for 1 full week.

2021 · HSE Ireland — Entire national health service affected. Disprution in some entities for months.

2022 · Centre Hospitalier Sud Francilien, France — €10M ransom demanded. Emergency department forced to redirect patients for weeks.

2024 NHS London, UK — Blood testing services affected; 10,000+ appointsments postponed. 1,700 procedures canceled. Patient harm documented. One **patient death** confirmed as contributing factor.

02 · The Next Wave

HIMSS 26

Five Emerging Threat Vectors

02 · THE NEXT WAVE

The threat landscape is shifting from opportunistic to strategic, AI-driven and automated.

1

AI-Powered Attacks

Autonomous phishing, deepfakes, and self-adapting malware at scale.

2

Medical Devices

Unpatched, networked IoMT devices as permanent attack surface

3

Quantum Computing

'Harvest now, decrypt later' as long term threat

4

Supply Chain

Third-party vendors as low-security entry points into medical networks.

5

Data & AI Governance

Patient data in AI training raises data raises sovereignty and adversarial-attack risks.

AI Attacks

AI enables hospital-specific phishing at massive scale with perfect grammar.
Deepfake voice/video: Impersonating executives or IT helpdesks.
Malware that adapts in real time to evade detection

AI-generated synthetic data poisons diagnostic models — wrong diagnoses at scale.

First Step: AI email filtering · MFA for all staff · deepfake awareness drills.

IoMT Risk

Connected devices — pacemakers, infusion pumps, MRI/CT, lab automation — often unpatched, networked, and running legacy firmware.
Ransomware disables imaging for days, cancels surgeries, forces paper-based care.
Building systems (HVAC, access control) increasingly connected and under-secured.

First steps: Segment IoMT networks · vendor security reviews · patch SLAs in procurement.

Quantum

Threat horizon: 5-10 years — but preparation must start now.
Current RSA/AES encryption is vulnerable to quantum brute-force.
'Harvest now, decrypt later': records stored today, decrypted once quantum matures.
Health records with 50+ year retention are particularly at risk.

First steps: Adopt NIST post-quantum standards (2024). Build your migration roadmap.

Supply Chain

Germany 2024: Pharma distributor AEP offline 1 week — 130+ hospitals affected.
Third-party lab, radiology and pharmacy systems: low-security entry points.
Vendors with privileged remote access to clinical systems: invisible attack surface.

First steps: Zero Trust architecture · vendor security assessments · contractual SLAs.

Data Sovereignty & AI Governance

EU AI Act · Adversarial AI · Data Sovereignty

- AI Training Data Risk: Patient data used to train models — ownership and storage must be contractually defined. Require EU-sovereign cloud.
- Adversarial AI Attacks: Manipulated inputs fool diagnostic AI — wrong diagnoses at scale. Mandate model validation, human-in-the-loop, red-team testing.
- EU AI Act (2026): Most medical AI is high-risk. Conformity assessments, transparency, explainability and EU AI database registration are mandatory.
- Without EU-sovereign cloud requirements, patient data risks leaving European jurisdiction.

03 · Policy & Governance

HIMSS 26

The Regulatory Wave — NIS-2 & Beyond

Compliance is a legal obligation — not an IT project

- **NIS-2 Directive:** Risk analysis and incident response plans mandatory — Supply chain security requirements — MFA and encrypted communications — 24-hour incident reporting to national authority — Executive management personally liable — Maximum penalty: EUR 10 million or 2% of global annual turnover
- **National implementation varies:** Germany (NIS2UmsuCG): named security officer, reporting to BSI — Check your country's transposition status and timeline
- **EU AI Act (enforcement from 2026):** Most medical AI classified as high-risk: conformity assessments, transparency and EU AI database registration required
- **Bottom line: NIS-2 is personal management liability. Name an accountable executive owner now.**

04 · Immediate Action Plan

HIMSS 26

Germany's €1.8 Billion Response

03 · POLICY & GOVERNANCE

Up to 4,000 facilities: hospitals, rehabilitation centres, outpatient clinics, pharmacies, laboratories ·

Funding via national development bank · Progress measured against 5-Level Maturity Model

1

2026

Baseline assessment: IT security status and strategy for all facilities. Flat-rate funding to get started.

2

2027

Emergency Measures: Critical security gap remediation. NIS-2 quick wins. Matched co-funding required.

3

2028

Core NIS-2 Readiness: Strategic long-term measures. Maturity Model Level 3+ target. Project-based funding.

4

2029

Advanced Resilience: Deep security integration. Supply chain coverage. Programme completion and audit.

Three principles that apply regardless of jurisdiction: start with an honest baseline, fund by maturity level, mandate progress over time.

Cybersecurity Is a Board-Level Responsibility

Regulation sets the rules. Your organisation must build the structure.

Structure It

- Direct reporting line: security lead to board
- Separate oversight from IT operations
- Quarterly board briefings wird standardises metrics
- Cybersecurity as a standing board agenda item

Measure It

- Current maturity level
- mean time to full recovery after major incident
- Percentage of systems unpatches beyond 30 days
- Date and result of last incident responce excercise

Fund It

- Treat cybersecurity as ist own budget category, separate from general IT
- Baseline assesment first, then investmetn by maturity level

→ If ransomware hit tonight, would your organisation know where it stands?

Translating Threats into Board Decisions

Five questiond for the next Monday Morning Board Meeting

- Questions for your CISO:
- What is our current cybersecurity maturity level — and when was it last independently assessed?
- If ransomware hit tonight, how long would full recovery take? Has this ever been tested?
- Which third-party vendors have privileged access to our clinical network — and when were they last audited?
- Do we have a dedicated cybersecurity budget — or is it buried inside general IT spending?
- When did we last run a full incident response drill?
- Who on our executive board is personally accountable for NIS-2 compliance — by name?

→ If the board cannot answer all five, the time to act is now.

05 • Key Takeaways

HIMSS 26

What to remember

Cybersecurity is not an IT problem. It is a patient safety problem.

- 1: The threat is evolving: AI-driven, automated, targeting supply chains and medical devices.
- 2: Regulation is here: NIS-2 makes leadership personally liable. No more delegation.
- 3: Start now: appoint an owner, assess your baseline, test your response.

HIMSS 26
EUROPE

Thank you