
Hospital Cyber Defence Course for Executives: Detection, Devices and Recovery with AI

13 – 17 December 2026
Sharm El-Sheikh





Hospital Cyber Defence Course for Executives: Detection, Devices and Recovery with AI

Ref: 694_34063 **Date:** 13 – 17 December 2026 **Location:** Sharm El-Sheikh **Fees:** 4000 GBP

Programme Summary

Hospital cyber defence is the subject of this one-week training course for hospital executives, security leaders and digital health managers, ending in a cyber resilience plan for one hospital. Clinical services now depend on connected devices, shared records and suppliers, and attackers use automation to reach them. The programme moves from risk to detection, devices, recovery and oversight of AI security tools, using cases from hospitals, laboratories and insurers. Mars Training Centre UK delivers this programme on hospital cyber defence to mixed-organisation cohorts.

The Business Case

When ransomware or a device fault stops a ward, the cost is measured first in delayed care and only later in money. Leaders who can rank clinical systems by harm, judge what AI detection can and cannot do, and rehearse recovery decide faster and explain their choices to boards and patients with evidence.

- Clinical Continuity: Improves as critical systems, downtime procedures and recovery order are agreed beforehand.
- Patient Data Exposure: Falls as access, logging and supplier controls are reviewed against actual data flows.
- Detection and Response Time: Shortens as alerts, escalation paths and decision rights are tested in rehearsal.

Principles and Evidence Base

- NIST Cybersecurity Framework: Provides the identify, protect, detect, respond and recover structure used to organise Sessions 1 to 4.
- HHS 405d Health Industry Cybersecurity Practices: Supplies health-specific threats and practices that shape the risk register built in Session 1.
- HIPAA Security Rule: Frames the safeguards for protected health information that are mapped to controls in Session 2.

Intended Participants

- Hospital executives who accept cyber risk on behalf of clinical services.
- Information security leads who must explain detection tools and incidents to non-technical colleagues.
- Digital health and information technology managers who buy, connect and support clinical systems.
- Clinical engineering and biomedical leads who look after connected medical devices.
- Risk, legal and continuity managers who prepare the response to a major incident.



Typical settings include hospital groups, health insurers, diagnostic laboratories and public health agencies.

Learning Outcomes

1. Participants will be able to prioritise clinical systems and data by the harm their loss would cause.
2. Participants will be able to diagnose weaknesses in access, supplier and device arrangements using a risk register.
3. Participants will be able to evaluate AI detection tools against false alarms, blind spots and data needs.
4. Participants will be able to construct a ransomware response and recovery sequence for clinical services.
5. Participants will be able to justify controls and oversight for AI security tools to a governing board.

Programme Structure

Day 1: Hospital Cyber Defence Risk and Clinical Priorities

Which systems and data matter most to patient care, and what threatens them?

- Clinical Service Dependency Map
- Patient Data Flow Inventory
- Threat Scenario Catalogue
- NIST Cybersecurity Framework Function Mapping
- Harm-Based Risk Register

Day 2: Access, Suppliers and Data Safeguards

Who can reach patient records and systems, and how is that proven?

- Privileged Access Review
- Supplier Connection Risk Questionnaire
- Safeguard to Control Matrix
- Logging and Audit Trail Standard
- Phishing Exposure Assessment

Day 3: AI Detection and Connected Medical Devices

What can AI detection see, and how are devices that cannot be patched protected?

- Anomaly Detection Use Cases
- False Alarm and Blind Spot Test
- Medical Device Inventory and Segmentation Plan
- Attacker Use of AI Briefing
- Detection Tool Selection Scorecard



Day 4: Ransomware Resilience and Recovery

How do services continue and return in the right order after an attack?

- Downtime Procedure Cards
- Backup and Restore Test Plan
- Recovery Priority Sequence
- Incident Decision Log
- Patient and Public Communication Statement

Day 5: Cyber Resilience Plan for One Hospital

Do the earlier records form one plan that leaders can run?

- Applying the Session 1 Harm-Based Risk Register
- Testing the Session 3 Detection Tool Selection Scorecard
- Rehearsing the Session 4 Recovery Priority Sequence
- Setting Oversight Rules for AI Security Tools
- Completing the Hospital Cyber Resilience Plan

Methodology

The programme uses a structured exercise method built on a shared case of a hospital group hit by ransomware through a supplier link. Participants work with prepared risk registers, alert samples and recovery timelines, then adapt each artefact to their own organisation and compare choices with peers from other sectors.

- Suggested activity: Ranking ten clinical systems by harm and agreeing the recovery order.
- Suggested activity: Judging a set of AI alerts and deciding which need escalation.
- Suggested activity: Briefing a board role-play on an overnight incident.

Capstone Output

Each participant completes a cyber resilience plan for one hospital. It holds a harm-based risk register, an access and supplier control list, a detection tool decision, a recovery sequence and an oversight calendar for AI security tools. The plan is used at work to brief a board, set supplier conditions and prepare an incident rehearsal.



Frequently Asked Questions

Is hospital cyber defence training suitable for executives without a technical background?

Yes. Hospital cyber defence is taught through cases and templates. It assumes experience in hospital management, clinical operations, risk or information technology, but no programming or security engineering skills.

Which frameworks does hospital cyber defence training rest on?

Hospital cyber defence training rests on the NIST Cybersecurity Framework, the HHS 405d Health Industry Cybersecurity Practices and the HIPAA Security Rule safeguards for health information.

How is the plan from hospital cyber defence training used at work?

You use the resilience plan to brief your board, set conditions for suppliers, choose detection tools and run a recovery rehearsal with clinical and technical teams.

How does hospital cyber defence differ from general cybersecurity awareness training?

Hospital cyber defence addresses clinical continuity, connected medical devices, patient data and AI security tool oversight, while general awareness training focuses on staff habits such as spotting phishing messages.