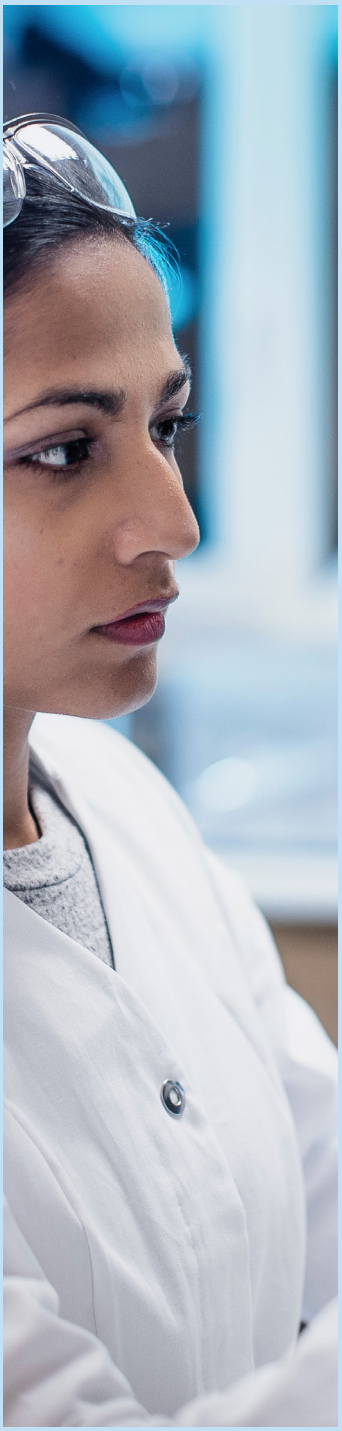
VIEW POINT



DEFENSIBLE CYBER POSITION IN HEALTHCARE: PROTECTING PATIENTS BEYOND THE DIGITAL REALM

Abstract

This POV explores how healthcare organizations can establish and maintain a defensible cyber position while ensuring continuous patient care.

In healthcare, cyber attacks can directly endanger human lives, not just information. We've seen ransomware paralyze hospitals, leading to delayed treatments and diverted emergency patients. Understanding this unique threat landscape is essential for developing effective security strategies that align with the sector's primary mission: patient care.

Infosys®
Navigate your next

The Unique Healthcare Cybersecurity Challenges

Legacy and Specialized Systems

Hospitals rely on network-connected medical devices often running outdated operating systems that cannot be easily patched or secured with traditional methods.

Patient Safety vs. Security Trade-offs

When availability means life-or-death, security measures that cause delays can negatively impact care, creating inherent tensions between protection and accessibility.

Limited IT Resources and Training

Many healthcare organizations operate with small IT teams, limited cybersecurity expertise, and clinical staff whose primary focus is patient care, not security protocols.

Regulatory Compliance Pressure

HIPAA and accrediting bodies like the Joint Commission mandate protection of patient data and continuity of care requirements that must be balanced with operational realities.

What is a Defensible Cyber Position in Healthcare?

Definition

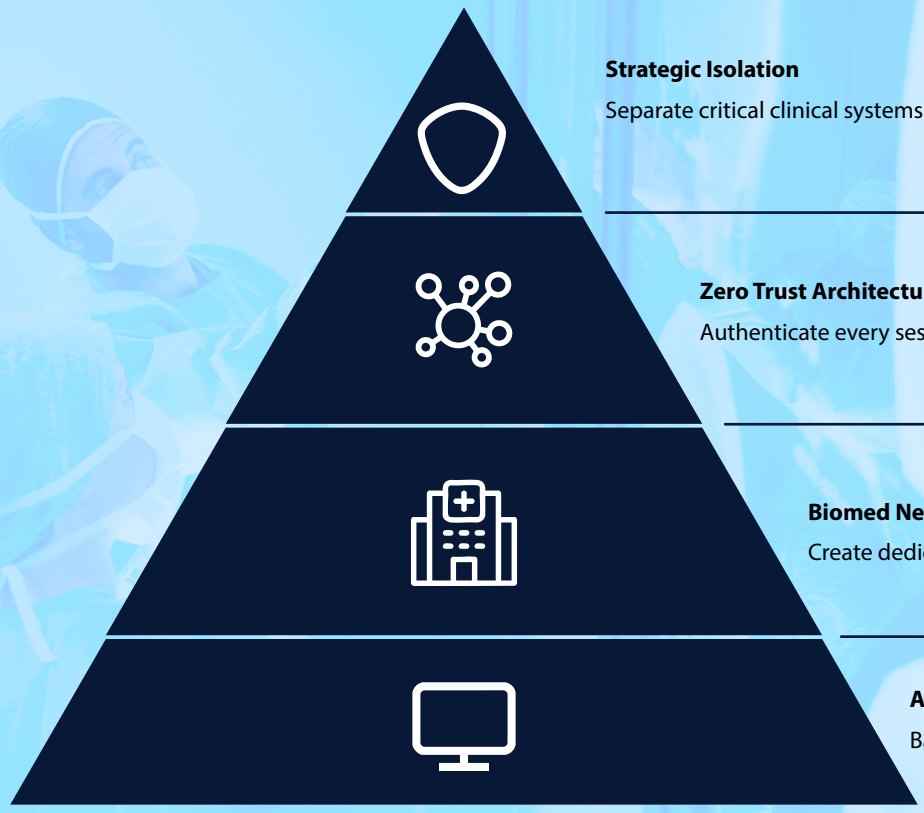
A defensible cyber position in healthcare means that even if clinical IT systems are compromised, the facility can continue critical patient care and protect life. It balances technological controls with operational continuity strategies.

This approach acknowledges that perfect security is impossible, but preparations for resilient operations during compromise are essential.

Key Components

- Network segmentation to contain threats
- Well-drilled procedures to switch to manual operations
- Isolated medical device networks
- Documented downtime procedures
- Regular practice of manual workflows
- Paper backup systems for critical information

Network Segmentation: The First Line of Defense



Strategic Isolation

Separate critical clinical systems from general networks

Zero Trust Architecture

Authenticate every session and limit lateral movement

Biomed Networks

Create dedicated networks for medical devices

Administrative Systems

Base-level segmentation for non-clinical operations

Modern hospitals implement network segmentation by isolating medical devices and high-risk systems from general hospital networks. For example, radiology machines and infusion pumps might reside on a separate VLAN or network segment, walled off by internal firewalls. If ransomware strikes the hospital's administrative network, it cannot easily jump to the medical device network.

Maintaining Care During IT Downtime

Prepare Downtime Kits

Maintain pre-printed forms, backup schedules, and instructions that can be quickly distributed when systems fail.

Develop Manual Workflows

Create detailed procedures for core clinical functions including medication administration, lab orders, and patient admissions without computers.

Regular Downtime Drills

Practice operating without electronic systems through simulated outages, building staff confidence and identifying workflow gaps.

Alternative Communication

Establish backup channels like analog phones or emergency radios when primary networks are compromised.

Tactical Incident Response in Healthcare

Detect and Assess

Quickly identify affected systems and determine potential impact on patient care. Engage clinical leadership immediately to assess care implications alongside technical issues.

Isolate and Contain

Segregate affected networks to prevent lateral movement. If ransomware hits one hospital in a multi-hospital network, isolate that facility while maintaining limited secure communications channels.

Activate Downtime Procedures

Implement manual operations using paper forms, whiteboards for tracking patient status, and runner-based communications. Deploy "downtime kits" with pre-printed materials and instructions.

Prioritize Critical Services

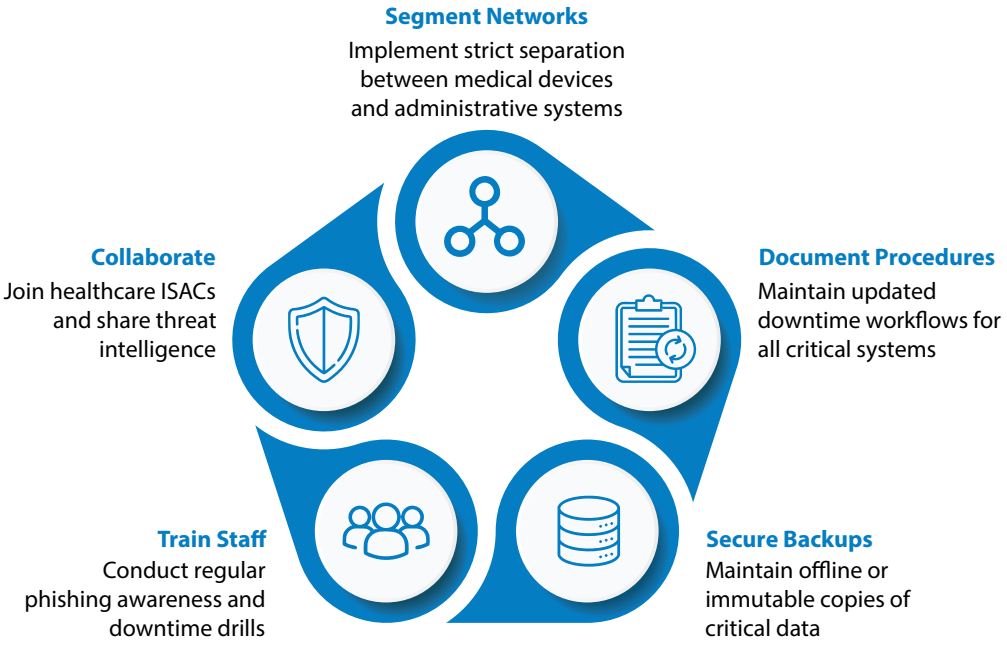
Triage hospital functions to ensure emergency and inpatient care continues while potentially postponing non-urgent appointments or elective procedures to focus resources.

Real-World Healthcare Cyber Incidents

Incident	Impact	Key Lessons
WannaCry (2017)	UK hospitals forced to divert ambulances; surgeries rescheduled	Network segmentation and downtime procedures were critical differentiators in recovery
Düsseldorf University Hospital (2020)	Emergency patient diverted to another hospital; patient died during delay	First reported ransomware-related death; inadequate network isolation and slow recovery processes
Universal Health Services (2020)	$67M financial loss but no patient harm reported	Effective offline documentation and manual workflows prevented clinical impact despite extended outage

The contrasting outcomes of these incidents demonstrate how preparation directly impacts patient safety. Hospitals with well-practiced downtime procedures and segmented networks minimized clinical disruption, while those lacking these measures experienced potentially life-threatening service interruptions.

Building Your Healthcare Cyber Resilience Strategy



Remember that cyber resilience in healthcare is fundamentally about patient resilience. Your investment in these areas not only protects against financial and reputational damage but directly supports your organization's healing mission. As the Joint Commission advises, hospitals must prepare to maintain clinical continuity for up to four weeks during cyber disruptions.

References

European Union & ENISA Resources

- European Commission
- Public Health - European Commission
- European Union Agency for Cybersecurity, ENISA
- Health-ISAC (Health Information Sharing and Analysis Center)

Standards & Frameworks

- ISO Health Informatics & Security Standards | ISO/IEC 81001-1:2021 – Security in Health Software | IEC/TS 81001 2 2:2025 – Health IT Security Controls
- NIST Cybersecurity Framework
- U.S. Department of Health & Human Services (HIPAA Security Guidance)
- ISA/IEC 62443 Standards for Industrial and OT Security
- How Hospital IT Security Compares to Industrial Automation Control System Security
- Healthcare Information Sharing and Analysis Center (H-ISAC)
- The Joint Commission – Standards and Emergency Management
- GDHP Guidance on Medical Device Cybersecurity
- CISA Healthcare & Public Health Cybersecurity Toolkit (USA)
- Infosys Cybersecurity Services

About the Author

Michel Bruggeman

Principal Consultant | EMEA IoT & OT Lead

Michel Bruggeman is a distinguished cybersecurity leader with over 25 years of experience, specializing in Operational Technology (OT) security, industrial cybersecurity architecture, and cyber resilience. He has held strategic roles across the insurance, manufacturing, energy, and semiconductor sectors, focusing on ICS/OT risk assessments, secure cloud adoption, and incident response readiness. Michel is a SANS /ISA Mentor and Microsoft Certified Trainer, with deep expertise in IEC 62443, DORA, NIS2, NIST, and ISO 27001.

For more information, contact askus@infosys.com

Infosys®
Navigate your next