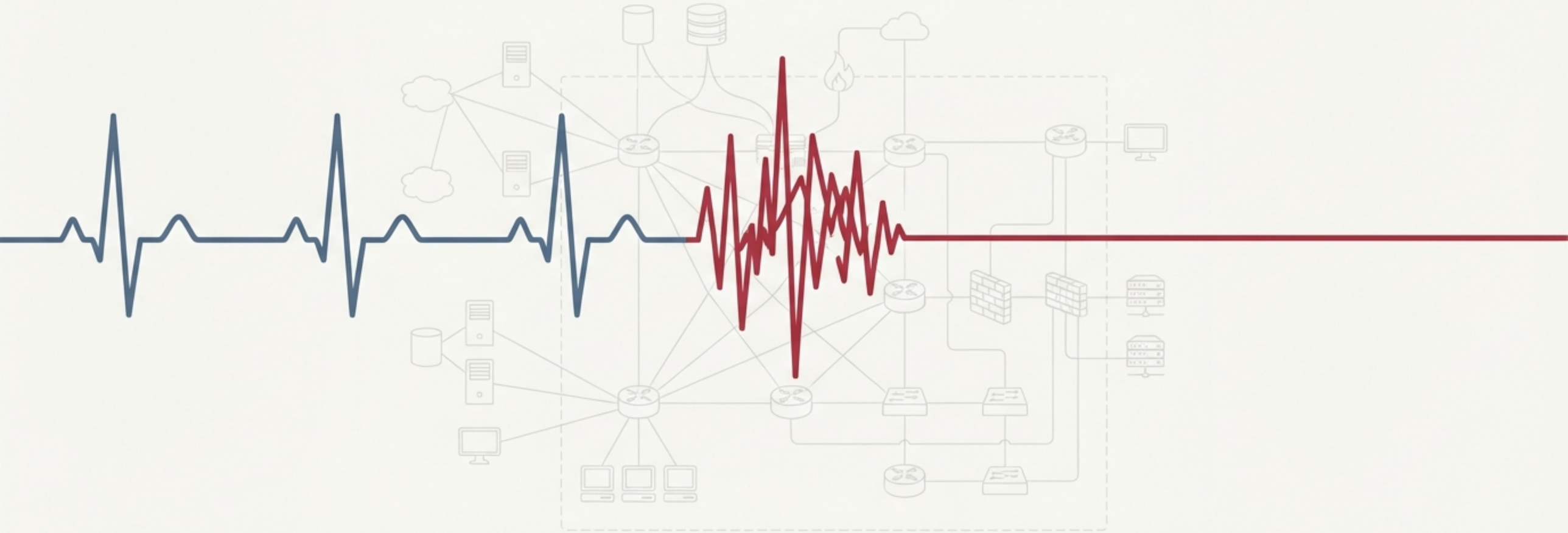
The Ascension Breach: A Blueprint for Cyber Resilience

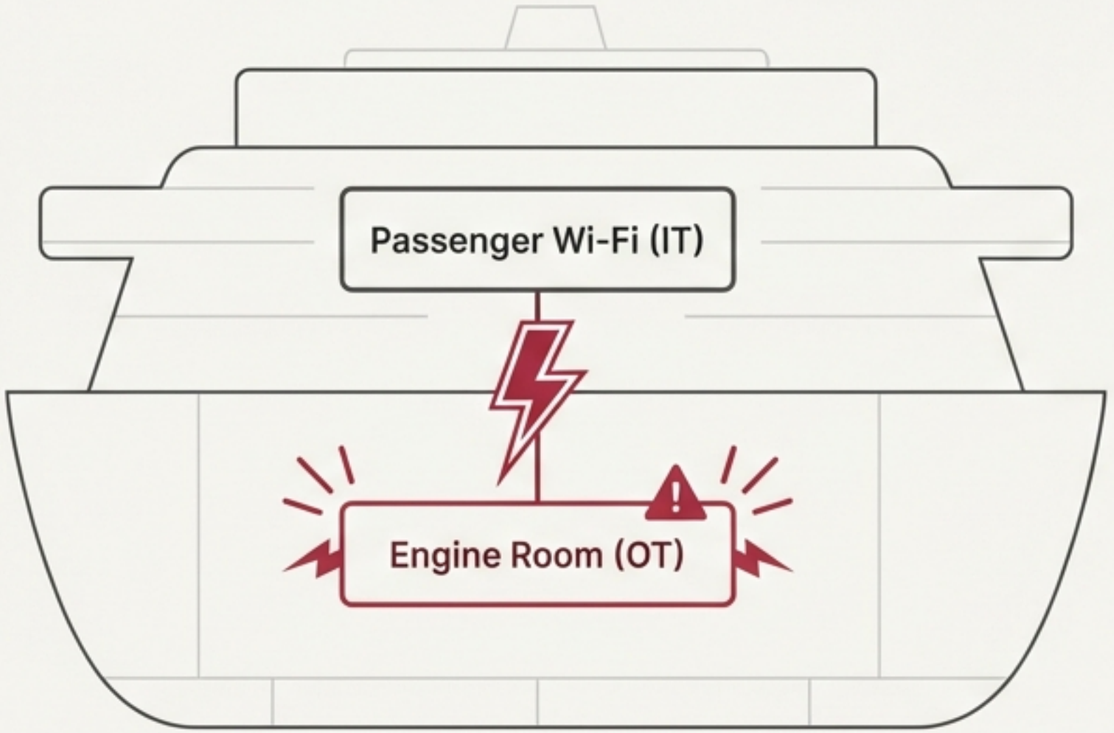
Lessons from a healthcare catastrophe and a strategic roadmap to OT/ICS maturity.



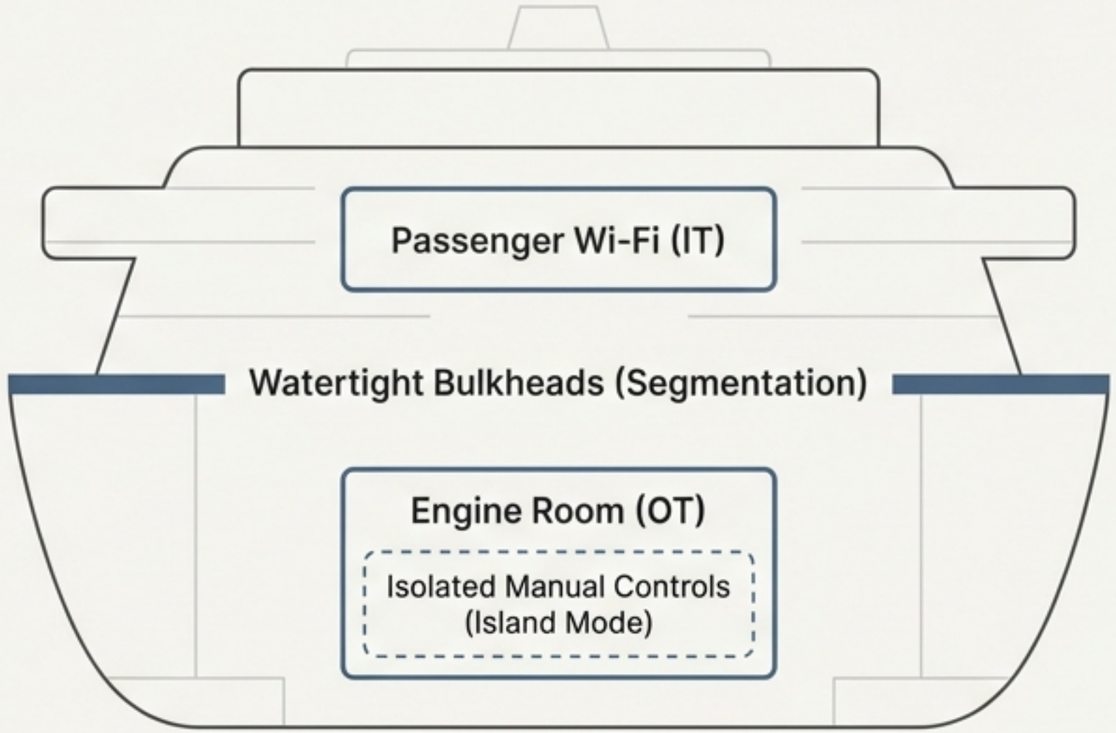
When the Passenger Wi-Fi Sinks the Ship

Ascension Health's crisis teaches a fundamental lesson: without deliberate separation, a compromise anywhere can become a catastrophe everywhere. They operated like a cruise ship where the **engine room (OT/Medical Devices)** was connected to the **passenger Wi-Fi (IT/EHR)**.

The Unsafe Ship

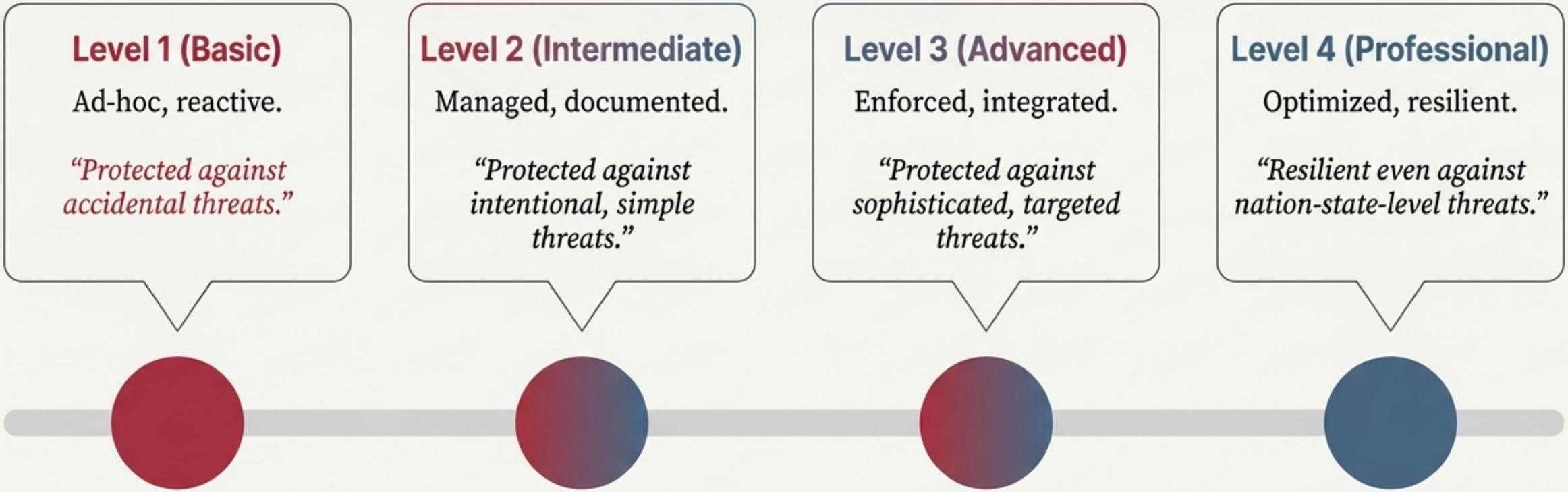


The Resilient Ship



Measuring Resilience: The OT Cybersecurity Maturity Model

Our goal is not just to fix individual vulnerabilities, but to systematically advance our organization's cybersecurity maturity. This journey is measured against a clear, four-level framework.



This model aligns with industry standards like IEC 62443.

The Diagnosis: Level 1 Defenses vs. a Level 3 Threat

The crisis was a catastrophic failure of security maturity. The attackers, Black Basta, operated with a sophistication aligning with **IEC 62443 Security Level 3 (SL-3)**. Ascension's defenses, however, were only prepared for coincidental violations, operating at **Maturity Level 1 (Basic) or IEC 62443 SL-1.**

Failure #1: The Collapsed Blast Radius

The Crisis

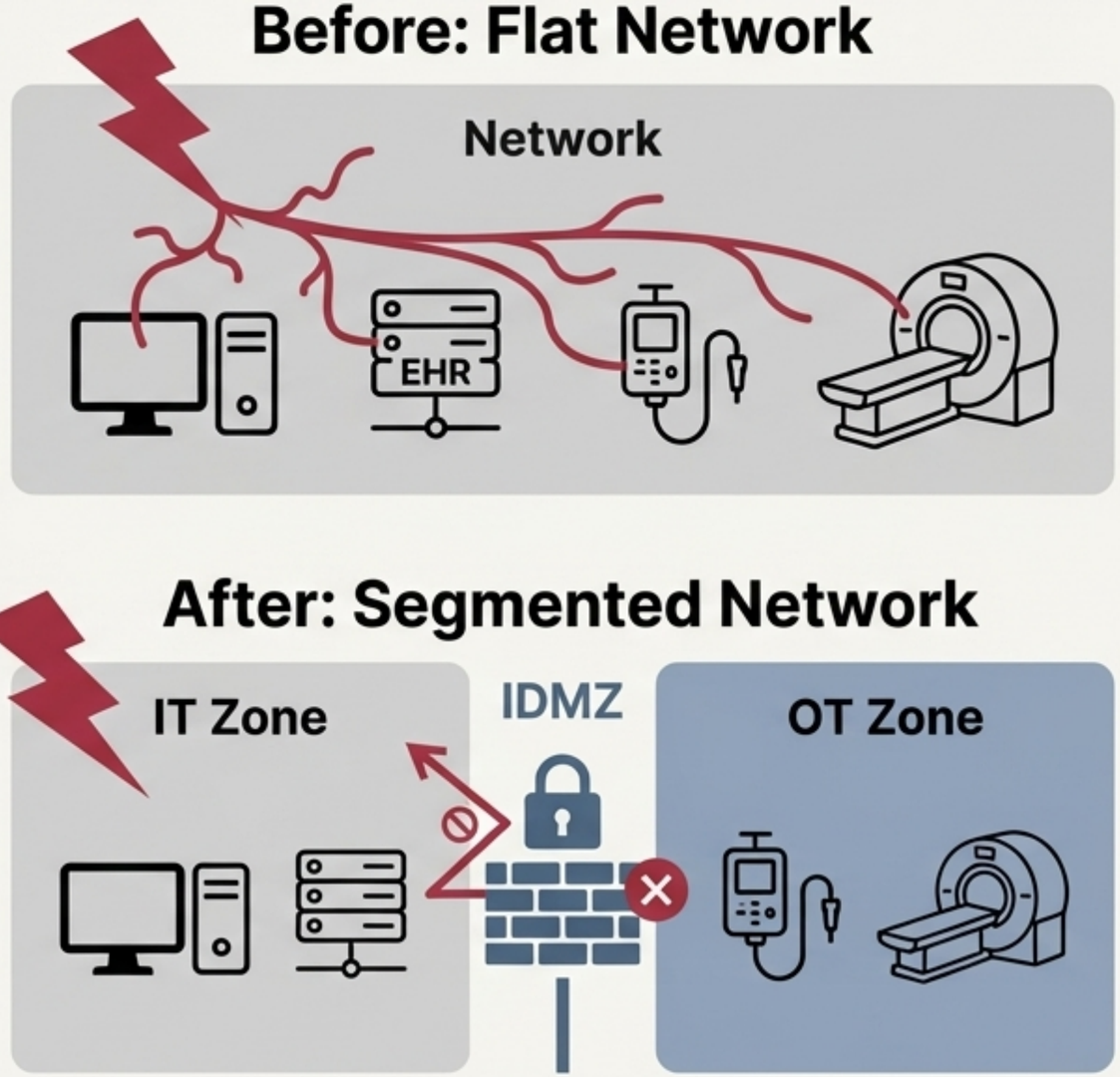
Ransomware entered the IT network (EHR) and immediately paralyzed critical OT assets like infusion pumps and scanners.

Maturity Diagnosis (Level 1)

The network was “flat.” IT and OT were bridged, allowing a threat on a corporate PC to directly impact the hospital ward. No effective **Industrial Demilitarized Zone (IDMZ)** was present.

The Lesson (Level 3 Goal)

Enforce strict separation between IT and OT using a firewall with a “Default Deny” policy, as defined by the **Purdue Model** and **IEC 62443 Zones and Conduits**.



Failure #2: The “Island Mode” Failure

The Crisis

With digital systems down, nurses resorted to using “paper runners” to transmit orders, bypassing critical digital safeguards like barcode scanning for medications and directly endangering patients.

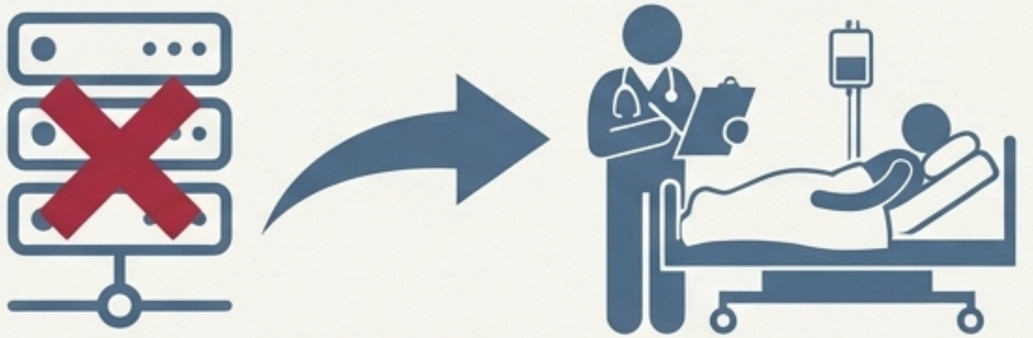
Maturity Diagnosis (Level 1/2)

The Business Continuity Plan was not “Decoupled.” It existed on paper but was completely dependent on IT systems to function, making it useless in an IT outage.

The Lesson (Level 4 Goal)

Engineer clinical processes to run safely *without* the digital overlay for a defined period. BCP must be about maintaining patient safety, not just restoring data. This is true **“Island Mode” capability.**

Failed BCP



Resilient “Island Mode”

Failure #3: The Human Firewall Failure

The Crisis

The attack likely initiated via credential theft from a phishing email. Staff were not trained to recognize the physical symptoms of a cyber-attack or how to respond.

Maturity Diagnosis (Level 2)

The organization relied on generic, annual "don't click links" training, which is ineffective against targeted Ransomware-as-a-Service groups.

The Lesson (Level 3 Goal)

Implement **Role-Based 'Cyber-Safety' Training**. Teach clinical staff to recognize a pump behaving erratically as a potential cyber incident—not just a mechanical failure—and to immediately revert to manual safety protocols.

Our Journey: From Reactive (Level 1) to Resilient (Level 3)

We will implement a 3-phase plan over 12 months to achieve OT Cybersecurity Maturity Level 3, aligning our defenses with the requirements of **IEC 62443 SL-3.**

Phase 1: Immediate Stabilization (Weeks 1-4)

Stop the bleeding and gain visibility.

Action 1: Deploy Passive Asset Discovery.

What: Install passive network sensors (e.g., Dragos, Nozomi, Claroty) on core switches.

Why: You cannot protect what you cannot see. This moves us from manual spreadsheets (Level 1) to continuous, automated monitoring (Level 3).

Action 2: Enforce Phishing-Resistant MFA.

What: Implement hardware-backed Multi-Factor Authentication (e.g., YubiKeys) for all remote and administrative access.

Why: Directly mitigates the credential theft vector used by Black Basta and other ransomware groups.

Phase 2: Architectural Hardening (Months 2-6)

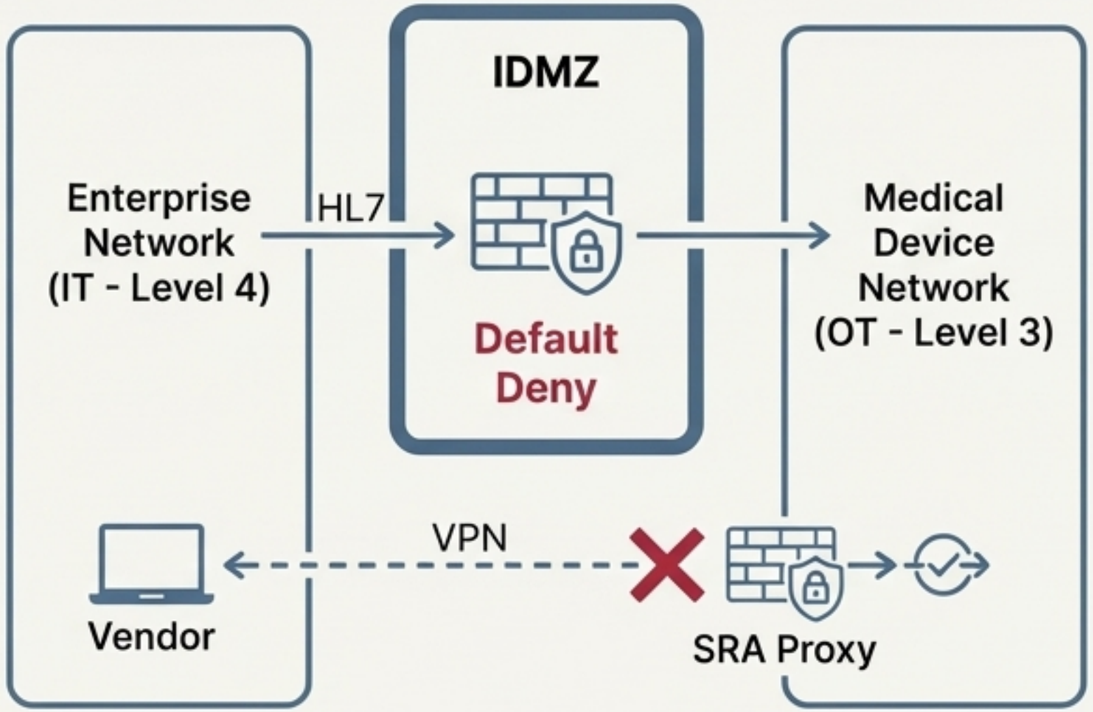
Objective: Build the watertight bulkheads using IEC 62443 Zones.

Action 1: Implement Purdue Model Segmentation.

- **What:** Erect a strict firewall boundary (IDMZ) between the Enterprise Network (Level 4) and the Medical Device Network (Level 3). Configure traffic policies to 'Default Deny."
- **Why:** Creates a barrier that allows OT to be safely isolated if IT is compromised. Only essential, filtered traffic (e.g., HL7) can pass.

Action 2: Implement Secure Remote Access.

- **What:** Eliminate direct vendor VPNs and implement a Secure Remote Access (SRA) proxy that "breaks the protocol."
- **Why:** Prevents a compromised third-party laptop from tunneling malware directly into the critical medical network.



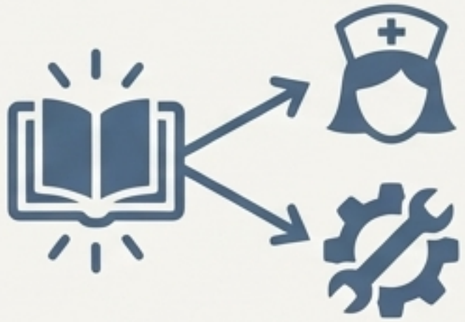
Phase 3: Resilience & Culture (Months 6-12)

Objective: Prepare our people and processes for the next attack.

Action 1: Conduct "Island Mode" Tabletop Exercises.

What: Run physical drills where the EHR-to-medical-floor connection is severed.

Why: Verifies that clinical staff can treat patients safely using manual procedures for at least 24 hours. This moves BCP from a "Paper Plan" (Level 2) to a **"Resilient Practice"** (Level 3).



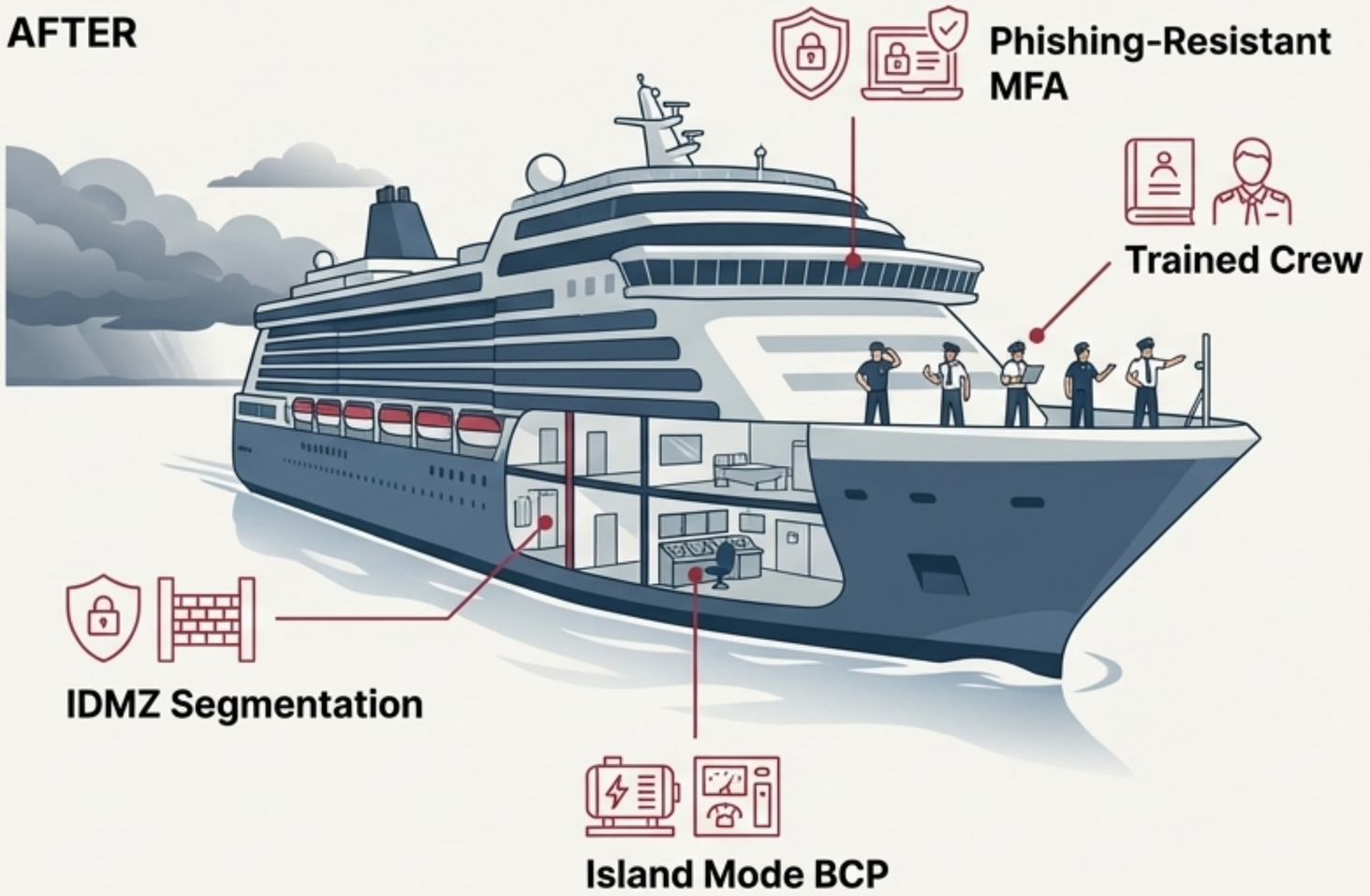
Action 2: Deliver Role-Specific Cyber-Safety Training.

What: Train clinical and engineering staff on the "Anatomy of an OT Attack."

Why: Empowers staff to recognize unexpected device behavior as a potential cyber incident and act decisively, making them a true first line of defense.

From a Single Point of Failure to a System Designed for Safety

This is not just about technology; it is about re-architecting our systems and culture to ensure patient safety is paramount, even during a cyber-attack.



Key Questions for Our Leadership

- Do we have a complete, continuously updated inventory of every medical device on our network, and do we know exactly what it's communicating with?
- Where are our "watertight bulkheads" between corporate IT and clinical operations? Could a compromised email server shut down our infusion pumps?
- Have we ever physically tested our ability to run in "island mode" for 24 hours? Is our BCP a real capability or just a document?
- Does our training prepare clinical staff for the physical reality of a cyber-attack, or is it generic compliance training?

Discussion & Next Steps

Project Lead Name / Department

[Internal Link to Project Charter/Documentation]