



IoMT is OT Cyber's Fastest Growing Blind Spot

Why Connected Medical Devices Now Represent Healthcare's Most Overlooked Cyber-Physical Risk

Thomas Jackson

IoMT is OT Cybers Fastest Growing Blind Spot: Why Connected Medical Devices Now Represent Healthcare's Most Overlooked Cyber-Physical Risk

Healthcare organizations are experiencing a paradigm shift driven by the rapid proliferation of connected medical technologies. The Internet of Medical Things (IoMT), a vast ecosystem of interconnected medical devices, sensors, and applications is transforming clinical care by enabling remote monitoring, predictive diagnostics, and real-time decision support. These technologies increasingly influence clinical decisions at the point of care, meaning their availability, integrity, and reliability are directly tied to patient health and safety.

However, this transformation has outpaced traditional cybersecurity frameworks and operational governance models, creating a critical blind spot at the intersection of IT, OT, and clinical engineering one where cyber incidents can quickly cascade into clinical disruptions and patient harm.

What is IoMT — and Why Are We Only Hearing About It Now?

The Internet of Medical Things refers to networked medical devices and associated software that collect, analyze, and transmit health data across clinical environments. These devices range from wearable patient monitors and infusion pumps to diagnostic imaging systems and smart implants. While the concept overlaps with IoT, IoMT is uniquely tethered to healthcare delivery and directly impacts patient outcomes and safety. ¹

Two forces drive today's attention on IoMT: **explosive market growth and rising vulnerability exposure**. The global IoMT market is projected to expand dramatically, with estimates showing growth from roughly \$97.7 billion in 2025 to over \$244 billion by 2029, illustrating the scale of adoption underway. ² By sheer ubiquity, healthcare delivery organizations (HDOs) can no longer consider these devices peripheral to clinical operations.

How IoMT Differs in Healthcare and Where Ownership Confusion Begins

Unlike traditional OT in industrial environments where ownership and risk governance are often clearly aligned with engineering and operations, IoMT sits in a *three-dimensional governance gap*. Clinical engineering manages device performance and patient safety; IT handles network, identity, and enterprise cybersecurity; and OT may be tasked with maintaining device operational continuity and system reliability.

This blurred ownership creates organizational ambiguity. Many IoMT devices:

- Operate outside clinical engineering's traditional scope,
- Are not visible to IT inventory tools,
- Are managed without any OT or engineering integration.

One survey highlights this challenge: in many hospitals, visibility into IoMT assets remains limited, and complete device inventories are a top cybersecurity pain point for CISOs. ³

IoMT Sits Between IT, OT, and Clinical Engineering

IoMT intersects all three domains:

- IT: Manages connectivity, identity, and network security.
- OT: Ensures device reliability, safety controls, and real-time operations.
- Clinical Engineering: Focuses on device efficacy, calibration, and regulatory compliance.

This triad often lacks a single accountable function, leading to governance gaps that adversaries can exploit. IoMT devices were traditionally excluded from OT risk assessments and hardening practices, leaving them exposed on healthcare networks and rarely segmented from core clinical systems.

IoMT does not cleanly belong to IT or OT it inherits risk from both while introducing patient safety consequences unique to healthcare. Unlike traditional IT systems or even classical OT systems, IoMT devices operate at the point of care, often outside standard cybersecurity visibility and governance models.

This creates a systemic blind spot where:

- IT assumes devices are “clinical”
- Clinical engineering assumes cybersecurity is “IT”
- OT assumes IoMT is out of scope

The result is fragmented ownership, inconsistent controls, and elevated risk.

Table: Key Differences Across IT, OT, and IoMT in Healthcare

| Dimension | IT (Healthcare IT) | OT (Healthcare OT) | IoMT (Internet of Medical Things) |
|------------------|---|--|--|
| Primary Purpose | Support business and administrative functions | Support facility and operational continuity | Directly support patient care and clinical decision-making |
| Typical Systems | EHRs, ERP, email, data centers, cloud platforms | Building automation (HVAC), power systems, medical gas, labs, pharma manufacturing | Infusion pumps, patient monitors, imaging systems, wearables, smart beds |
| Primary Priority | Confidentiality of data | Availability and reliability | Patient safety, availability, and data integrity |
| Failure Impact | Data breach, operational disruption | Facility outage, care disruption | Direct patient harm, care delays, clinical risk |

| | | | |
|-----------------------------|------------------------------------|--|--|
| Operational Characteristics | Patch-friendly, short lifecycles | Long lifecycles, deterministic control | Long lifecycles, software-driven, safety-critical |
| Change Tolerance | High (frequent updates) | Low (strict change control) | Very low (clinical validation required) |
| Connectivity Model | Enterprise network, cloud-first | Segmented industrial networks | Enterprise + OT + cloud + vendor remote access |
| Cybersecurity Model | IT security stack (EDR, SIEM, IAM) | Defense-in-depth, zoning, resilience | Hybrid IT/OT model with clinical safety constraints |
| Typical Ownership | IT / CIO organization | Facilities / Engineering / Operations | Clinical Engineering (device), IT (network), OT (availability) |
| Accountability Gap | Generally well defined | Generally well defined | Often unclear or fragmented |
| Regulatory Drivers | HIPAA, HITECH | Life safety codes, operational regulations | FDA, patient safety, privacy, emerging cyber mandates |
| Security Tool Coverage | Mature and standardized | Improving but uneven | Often limited or incomplete |

Why IoMT is a Critical Blind Spot in Healthcare

The risk is not theoretical. Recent data reveal alarming exposure levels:

- Hospitals are nearly universally exposed to exploitable IoMT vulnerabilities, with some reports showing 99 % of healthcare networks contain at least one IoMT device with a known vulnerability.⁴
- On average, IoMT devices carry 6.2 vulnerabilities per device, and around 60 % are end-of-life and no longer patched by manufacturers, increasing persistent risk.⁴
- Healthcare environments have massive, connected *footprints*, with some hospitals reporting hundreds of thousands of connected devices, many of which are unmanaged or unknown.⁵

This environment has serious operational and safety implications. A compromised infusion pump or patient monitor is not just an IT breach it is a patient safety incident with operational and clinical consequences.

Governance Gaps Amplify Risk

Traditional cybersecurity governance often places IoMT in a technology silo within IT or clinical engineering, leaving strategic oversight disconnected from OT and patient safety risk management. This fragmentation results in:

- Lack of comprehensive asset inventories,

- Inadequate segmentation between clinical networks and corporate systems,
- Unclear accountability for vulnerability remediation,
- Absence of threat modeling tied to clinical outcomes.

These governance gaps mirror classic OT cyber challenges, where ambiguity in ownership has historically delayed identification and treatment of risk. Healthcare must embrace similar accountability structures against IoMT risk.

Why Traditional OT Security Models Need Adaptation

Traditional OT security paradigms focus on deterministic control systems, safety interlocks, and engineered protections principles not initially designed for heterogeneous, software-driven IoMT ecosystems. Many IoMT devices:

- Run on proprietary operating systems with limited patching options,
- Communicate over Wi-Fi or Bluetooth, increasing attack surfaces,
- Interface with cloud platforms and third-party services.

These characteristics require a hybridized security model that blends OT resilience with IT and clinical risk controls, including:

- Zero-trust segmentation tailored for IoMT network behavior,
- Continuous inventory and vulnerability monitoring,
- Vendor accountability for security updates and lifecycle management, and
- Cross-functional governance bridging cybersecurity, clinical engineering, and operations.

What Needs to Be Adapted — A Strategic Framework

To close the IoMT blind spot, healthcare organizations need an **IoMT risk governance framework** that aligns to OT and cyber best practices:

1. **Unified Asset Management:** Integrate IoMT devices into enterprise and OT inventories for full visibility.
2. **Segmentation & Zero Trust:** Apply network isolation and micro-segmentation to limit lateral movement.
3. **Cross-Disciplinary Governance:** Establish executive oversight spanning OT, IT, and clinical engineering.

4. Risk-Driven Patch and Lifecycle Policies: Prioritize IoMT devices based on safety impact and exploitability.
5. OT-Informed Vulnerability Prioritization: Use OT risk scoring to inform IoMT patching and mitigation workflows.⁶
6. Continuous Monitoring and Anomaly Detection: Leverage analytics tuned to clinical protocols and device behavior.

This hybrid approach mirrors advanced OT cybersecurity practices but acknowledges the clinical and patient safety dimensions unique to IoMT.

Bringing Strategy, Trust, and Revenue Impact Together

For healthcare organizations and their technology partners, addressing IoMT is not just a security imperative, it is a strategic differentiator. Executives who can deliver secure, resilient IoMT ecosystems will:

- Improve operational efficiency and patient outcomes,
- Reduce the likelihood of high-cost breaches,
- Strengthen trust with patients and regulators,
- Create new revenue opportunities tied to secure digital healthcare services.

Being ahead of the IoMT blind spot reinforces an organization's reputation for patient safety and continuous care delivery a powerful competitive advantage.

Closing Thoughts

IoMT has quietly become healthcare's fastest-growing operational exposure not because it is inherently insecure, but because it has evolved faster than the governance, ownership models, and cyber-physical security frameworks designed to protect patients and operations. As connected medical devices proliferate across care delivery environments, IoMT now sits at the convergence of clinical care, operational reliability, and cybersecurity risk.

The challenge facing healthcare leaders is no longer whether IoMT delivers value it clearly does, but whether organizations are prepared to govern it with the same discipline applied to other safety-critical systems. Treating IoMT solely as an IT problem overlooks its operational dependencies and patient safety implications. Treating it as a traditional OT problem ignores its clinical workflows, regulatory obligations, and dynamic connectivity. IoMT demands a hybrid approach that bridges IT, OT, and clinical engineering under clear executive accountability.

Organizations that integrate IoMT into OT cyber frameworks establishing clear ownership, enforcing resilience-by-design, and aligning cyber controls to patient safety outcomes will be better positioned to

reduce risk, support clinical innovation, and build trust with patients, regulators, and partners. Those that do not will continue to operate with a growing blind spot one where cyber incidents can quickly become clinical events.

Ultimately, IoMT is not just a technology challenge; it is a leadership challenge. The healthcare organizations that address IoMT as both a clinical asset and an OT-cyber risk will unlock its full potential safely, responsibly, and at scale.

“IoMT: Where Cyber Risk Becomes Patient Risk.”

Resources

1. Internet of Medical Things: A systematic review, *ScienceDirect*, Neucom.
2. “Internet of Medical Things Market Growth and Trends 2025 ...” *Citrusbug Blog*.
3. “Hospital Cybersecurity Trends 2026: Top IoMT Challenges ...” *HIT Consultant*, Dec 18 2025.
4. “IoMT Vulnerabilities Statistics & Security Trends 2025.” *DeepStrike.io Blog*.
5. “Healthcare and Medical Device Cybersecurity Risk Statistics for 2025.” *C2A-SEC*.
6. “Vulnerability Prioritization for IoMT Security.” *Asimily Blog*.

Tom Jackson is a senior OT/ICS cybersecurity executive with 20+ years of experience helping regulated and critical infrastructure organizations move OT cybersecurity programs beyond assessment into execution, resilience, and measurable business outcomes.