Healthcare CIO and CISO Checklist for Wireless IoMT Security

At the center of digital transformation initiatives inside Healthcare Delivery Organizations (HDOs) is the connectivity of medical solutions.

For many HDOs, the ability to access and leverage real-time information can enable faster and more efficient decision making, evidence-based care, and the elimination of errors, while also reducing the overall cost of care.

This push for connectivity, together with the rise of IoT (Internet of Things) and IoMT (Internet of Medical Things) and the consumerization of healthcare, is driving the deployment of an unprecedented number of digital devices and wireless technologies in care environments — including wireless telemetry (patient monitoring) and MedRadio (wireless controlled pacemakers, defibrillators, muscle stimulators, and the like), among many more.

> "It has become crucial for our industry to accelerate our advancement of wireless IoT security for medical devices. Visibility into wired and wireless environments in all aspects of device and data management is critical to protect privacy and provide confidence in their facilities, whether at home or when in transit. Any deviation from standard protocols should provide a proactive alert and reduce any impact from an unacceptable vulnerable condition, allowing companies to enforce zero trust policies."
>
> **— Craig Richardville, CIO, SCL Health**

Health delivery organization CIOs and CISOs are responsible for securing these devices against intrusion and mitigating risk as part of a cybersecurity strategy. Yet, as a recent Gartner report notes, HDO CIOs and CISOs lack a complete and accurate inventory of devices in their environments. This significantly hinders their ability to continuously protect health delivery environments and secure medical data from attacks. Often, it is wireless IoMT devices — those enabled via cellular, Zigbee, WMTS, MedRadio, and the like — that pose a particular challenge, as they are not often connected to traditional wired-side HDO networks. As a result, CIOs and CISOs have significant cybersecurity blind spots and vulnerabilities, many of which they have no knowledge of.

To help CIOs and CISOs protect sensitive medical data and detect cyber threats involving IoMT and IoT devices, we have prepared a CIO Checklist for broad spectrum wireless IoMT Security. Using this checklist, CIOs and CISOs can assess their readiness for securing wireless devices and further harden their security posture against all manner of IoMT and IoT threats.

> "In healthcare, availability and uptime are critical — and life-threatening to patient care — if not protected. This challenge is compounded due to the high number of endpoints (medical equipment, cell phones, iPads, tablets, Fitbits, etc.) connected to both trusted & untrusted networks across wired and wireless protocols. Visibility and detection, therefore, have become essential. There is no "prevention" for healthcare organizations — there is only detect and respond. If you do not know what your environment is doing, you are blind. LOCH can help provide that visibility across multiple ranges; especially as most medical devices do not transmit in the standard 802.11 range."
>
> **— William Worthington, former CIO, Cottage Health**

1. Gain comprehensive IoMT and IoT visibility

CIOs and CISOs cannot protect what they cannot see. With the number and variety of IoMT and IoT devices expanding rapidly, along with the range of wireless frequencies on which they operate, security blind spots are larger than ever. HDO CISOs and CIOs must gain the ability to perform continuous asset discovery throughout the care environment to build a comprehensive understanding of every wireless device in operation — including devices that may not be managed by the HDO. Many IoMT devices communicate off-network and/or via side channels like cellular connections or other LPWAN radio frequencies, which means that monitoring traditional wired-side networks alone is not sufficient. Organizations must also conduct passive monitoring of the environment across broad-spectrum wireless and the mobile edge.

2. Assess known device vulnerabilities

Second, HDO CIOs and CISOs must work to understand the specific security gaps presented by every wireless IoMT and IoT device — regardless of whether they are WiFi-enabled, connected via cellular backhaul, via Bluetooth, or another LPWAN protocol. These vulnerabilities include not only those of individual devices, but those relating to the mobile edge or network infrastructure itself, to which devices are connected. Identifying, pinpointing and terminating rogue devices is mandatory; at the same time, passive monitoring of the RF spectrum should also identify bad actors that are creating DDOS scenarios with jamming or interfering RF signals — thus preventing any quick and easy access to critical patient telemetry information.

3. Rank and prioritize security threats by severity

Any device threats and vulnerabilities that are identified must be prioritized by their severity and impact to life, compliance, and business. As such, CIOs and CISOs must insist on data and event presentation in a manner that distills down the noise and drives lower mean-time-to-repair (MTTR) and the overall efficiency of cybersecurity operations.

4. Automate incident response

Finally, to enable rapid, scalable incident response across HDO environments, CIOs and CISOs must deploy automation. This can include everything from security alerts to fully automated incident response, including strategies like network fencing/segmentation, air termination, firewalls, command and control blocks, and more. In keeping with this strategy, CIOs and CISOs should also enable integrations between these wireless cybersecurity mechanisms and their existing SOAR and SIEM platforms — allowing them to automate the remediation process. Further, integrations with MDM/EMM tools can provide a much-needed ability to correlate threats and enable closed loop tracking and effective anomaly detection.

"With 80% of new IoT deployments now wireless, wireless has fast become the new network and new attack surface. It's important that we stay ahead of the curve by adopting innovative solutions that address the new threat landscape — misconfigured wireless devices can lead to data exfiltration and breach if not identified quickly. This is even more important for healthcare, as everything connected needs to be protected. LOCH's wireless security is unique in that it covers both broad-spectrum IoT as well as cellular IoT visibility and protection. Having deployed and used their mission-critical security solutions for over a decade now, I trust their products completely. A must-have in the toolbox."

— Rick Orloff, CEO of CSO Advisors

"Maintaining responsibility for all aspects of information security across a healthcare organization today is quite a daunting task. With so many wireless connected medical devices, it can be hard to know what telemetry data (PHI) is being transmitted and whether it is secured. Moreover, with the rapid adoption in WMTS (Wireless Medical Telemetry Services) and MedRadio communicating over non-standard frequencies, it is no longer adequate to just monitor standard WiFi. In my experience, these communications often never show up on the wired-side. LOCH has helped us check the cellular and full-spectrum wireless IoT security box, so I can move on to other things."

— Howard Haile, Chief Information Security Officer, SCL Health]

Summary

Even as the challenge of securing IoMT and IoT devices grows, there are steps that HDO CIOs and CISOs can take to reduce risk in their environment and stay ahead of the curve. By following the points in this checklist, healthcare CIOs and CISOs can establish robust IoMT cybersecurity processes and help ensure the protection of protected patient data.

For more information on securing the healthcare IoT and IoMT landscape, please see our white paper, Healthcare IoMT: A Review of Invisible Cyber Risks and Countermeasures.

Or visit us at loch.io

Interested in a Free IoMT Vulnerability Assessment?
Visit: https://lp.loch.io/vulnerability_assessment_offer

info@loch.io | 1-888-725-9434 | www.loch.io