

THE MONTHLY PULSE

March 2026

MedTech cybersecurity intel for engineering, quality & regulatory teams.

Published April 1, 2026

IN THIS ISSUE

- 01 From the Editor**
- 02 Upcoming event — MedTech World North America 2026**
- 03 Ask the Goat — the best cybersecurity move for legacy devices**
- 04 Podcast spotlight — Episode 61**
- 05 Medical device cybersecurity news — March 2026**

About this edition. Stryker's global shutdown, CISA endpoint guidance, and a cybersecurity-driven FDA recall — plus designing devices clinicians will actually use. Sourced from the Blue Goat Cyber LinkedIn newsletter, The Monthly Pulse.

THE MONTHLY PULSE

March 2026

Stryker's global shutdown, CISA endpoint guidance, and a cybersecurity-driven FDA recall — plus designing devices clinicians will actually use.

01

From the Editor

Cybersecurity is now deciding whether medical technology succeeds or fails. From disruption to regulation, March showed why MedTech can no longer afford to get security wrong. A major cyberattack disrupted MedTech operations, regulators tied security flaws directly to patient risk, and the pressure to get cybersecurity right continues to rise. The biggest issue we see: companies still treat cybersecurity too narrowly and too late. It is not just about the device — it is about the entire ecosystem, and building security into the product from the start.

02

Upcoming event — MedTech World North America 2026

May 11–13 at the Hilton West Palm Beach, FL. Blue Goat Cyber is Title Sponsor. The agenda spans capital strategy, commercialization, regulatory pathways, and innovation across neuro, cardio, robotics, and women's health. Christian Espinosa will speak on MedTech cybersecurity across the total product lifecycle. Use code **MTWUXCHRISTIAN** for \$150 off your ticket.

03

Ask the Goat — the best cybersecurity move for legacy devices

Awareness. The goal is not forcing modern controls onto outdated hardware — it is understanding real-world risk. Penetration testing shows how the device can actually be attacked today. An SBOM highlights third-party software exposure. A strong postmarket cybersecurity plan defines how you monitor, assess, and respond once the device is in the field. The key is a holistic, collaborative approach that prioritizes security throughout the entire product lifecycle.

04

Podcast spotlight — Episode 61

How to Design Devices That Integrate Into Clinical Workflow Without Disruption, with Prof. Aamer Ahmed. Too many medical devices fail for a simple reason: they were built before truly understanding the problem. Involving Key Opinion Leaders early isn't optional — it's essential. The episode covers what happens when companies skip this step, why seamless integration into clinical workflows is the difference between success and failure, and how AI-driven decision support and digital twins are reshaping care without removing physician accountability.

05

Medical device cybersecurity news — March 2026

bullet **Stryker cyberattack (March 11)** caused a global operational shutdown — disrupting manufacturing, order processing, and shipping without directly impacting devices in hospitals. Reports linked the attack to an Iran-aligned group targeting enterprise systems, with downstream risk to healthcare delivery and supply chains.

bullet **CISA issued urgent guidance** for medical device manufacturers following Stryker — harden endpoint management systems, enforce least-privilege access, and tighten control over tools like Microsoft Intune. Attackers are increasingly exploiting trusted IT management tools as a high-impact attack vector.

bullet **FDA Class II recall** for GE HealthCare's Centricity Universal Viewer over a cybersecurity vulnerability that could expose user credentials and allow unauthorized access. More than 2,000 systems worldwide are affected. Cybersecurity flaws are now triggering regulatory recalls — not just IT alerts.

Get the next Pulse in your inbox.

One email a month. MedTech-only. Read every edition at bluegoatcyber.com/resources/pulse or book a strategy session at bluegoatcyber.com/contact.