BLUE GOAT CYBER

www.bluegoatcyber.com

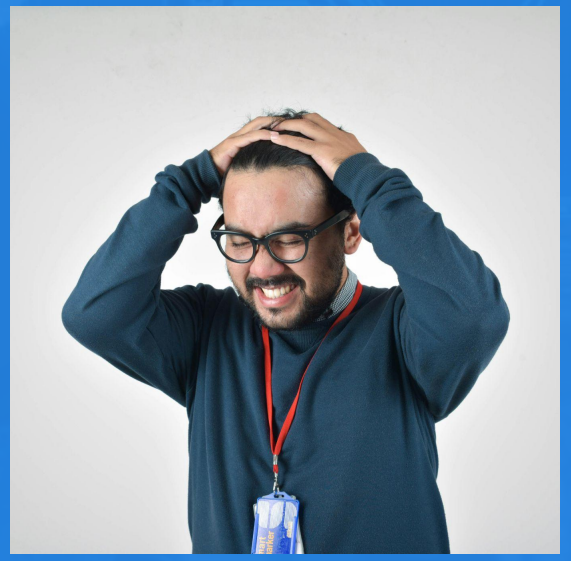
Cybersecurity & Lessons Learned from CDRH FDA Software Reviewers

Presented by Christian Espinosa, Founder and CEO

Protect Your MedTech Innovation from Regulatory Roadblocks

BLUE GOAT CYBER

Imagine you've spent 5 years and $20 million developing a life-saving device. You're ready to launch... but then the FDA rejects your submission.



The reason? Cybersecurity deficiencies. You're now facing months—or even years—of delay while competitors rush ahead.

This happened to ACME Systems.

When the FDA rejects you, it's not just paperwork. It's millions lost. It's patients left waiting.

What is the Real Cost?

Metric		Input	Notes
Average Monthly Revenue at Risk (due to FDA delay)	$	300,000	
Estimated Delay Time Avoided (in months)	$	3	
Estimated Time Saved by Team (hours)	$	2,080	Team of 4 fulltime, 13 weeks
Average Internal Hourly Rate (with overhead)	$	85	
Cost of Internal Effort Avoided	$	176,800	Hourly Rate x Hours
Estimated Submission Delay Avoided (Cost)	$	900,000	Monthly Revenue Lost x Months
Total Cost to Client	**$**	**1,076,800**	
Blue Goat Cyber Investment	$	150,000	
Net ROI (Cost Avoided - Package Cost)	**$**	**926,800**	
ROI Multiplier		**6.18**	

By the End of This Session, You Will...

✅ Understand the FDA CDRH's cybersecurity expectations for medical device submissions.

✅ Learn key cybersecurity deficiencies that trigger FDA RTA or major deficiency letters.

✅ Identify how cybersecurity gaps delay or derail FDA approvals.

✅ Gain a 3-step blueprint for developing FDA-ready cybersecurity documentation.

Your Market Leadership is at Risk

⚠️ Cybersecurity non-compliance leads to FDA RTA (Refuse to Accept) and major deficiencies

⚠️ Cybersecurity gaps directly link to patient safety risks

⚠️ Deficiencies cause 6–18 month clearance delays and market setbacks

Cybersecurity deficiencies are now the #1 reason for FDA premarket submission failures.

Top 5 Cybersecurity Deficiencies Identified by CDRH Reviewers

1. Missing or incomplete **threat modeling**
2. Inadequate or absent **Software Bill of Materials (SBOM)**
3. Cybersecurity risk management NOT tied to **exploitability and patient safety**
4. Late cybersecurity integration - **no SPDF (Secure Product Development Framework)**
5. Lack of independent 3rd party **penetration testing**

The #1 Reason MedTech Startups Stall: Cybersecurity Neglect.

FDA Deficiency Examples

Based on the information provided in your "Software Cybersecurity Repor[redacted], your device meets the definition of a cyber device under Section 524B(c) of the Federal Food, Drug, and Cosmetic Act. However, you did not provide threat modeling documentation. Threat modeling

Based on the information provided in the document Software Cybersecurity Report , your device meets the definition of a cyber device under section 524B(c) of the Federal Food, Drug, and Cosmetic (FD&C) Act. However, you did not provide a software bill of materials (SBOM), including commercial, open-source, and off-the-shelf software components as required by section 524B(b)(3) of the FD&C Act.

You provided security testing in your submission, however, the testing did not include vulnerability testing and penetration testing. Adequate cybersecurity testing is important to comply with the requirements specified in section 524B(b)(2) of the Federal Food, Drug, and Cosmetic Act to provide a reasonable assurance that the device and related systems are cybersecure. Verification and validation

The Origin of Blue Goat Cyber – A Mission to Secure MedTech

- About Christian Espinosa
- Involved with medical device cybersecurity since 2014
- Sold first cybersecurity company, Alpine Security, in 2020
- Health scare in Feb 2022…formed Blue Goat Cyber

CONCLUSION:

Acute deep vein thrombosis (DVT) in the left femoral, left popliteal, left gastrocnemius, left posterior tibial, left peroneal, left soleal veins. There is no evidence of superficial vein thrombophlebitis (SVT) in the proximal saphenous veins.

What if that doppler ultrasound device had been recalled due to cybersecurity issues?

MedTech cybersecurity failures = Delays, lost revenue, investment risk, and patient harm.

About Blue Goat Cyber

- Guided hundreds of manufacturers through FDA premarket submissions and deficiency responses
- Worked with every category of medical devices, such as:
  - Simple to Complex IVD systems
  - AI-Enabled SaMD
  - Blood Glucose Monitors & Insulin Pumps
  - Remote Patient Monitors & Wearable ECGs
  - Implanted Cardiac Devices (Pacemakers, Defibrillators)
  - Ventilators & Critical Care Machines
  - Networked Surgical Robots & Deep Brain Stimulators
- **100% Success Rate**
- **FDA-Clearance Guarantee**

3 Steps to Build an FDA-Ready Cybersecurity Program

1. Identify cybersecurity risks early and tie them to **patient safety impacts**
2. **Design cybersecurity controls** aligned with FDA Premarket Cybersecurity Guidance
3. Implement **lifecycle cybersecurity plans** for postmarket monitoring and vulnerability management

Case Study: Cybersecurity Oversight Leads to Regulatory Delay

The Manufacturer's Vision

✅ A bronchial decongestion device that transmits real-time patient data to the cloud for remote monitoring.

✅ Positioned as a next-gen connected medical device with AI-driven analytics for providers

The Cybersecurity Oversight

⚠️ Cloud-connected bronchial device **lacked secure boot** and firmware integrity

⚠️ Blue Goat Cyber's premarket submission review identified major vulnerability **70 days before planned submission**

⚠️ Emergency product pivot delayed submission and weakened market competitiveness

Emergency Pivot to Address FDA Cybersecurity Deficiency

FDA pre-submission review identified missing secure boot and firmware validation

- **Cloud-based features disabled** to satisfy minimum cybersecurity requirements
- **Pivoted product features** to minimize cybersecurity exposure
- Design changes and retesting **delayed FDA submission by 3 months**

Key Takeaways for Regulatory Affairs and Quality Teams

✔ **Engage cybersecurity early** to avoid FDA RTA and deficiencies

✔ Build secure hardware and software architectures **from the requirements & design phase**

✔ Document cybersecurity risks tied directly to **patient safety impacts**

✔ Implement real-world cybersecurity **penetration testing before submission**

✔ Prepare a comprehensive **postmarket cybersecurity management plan**

Case Study: Early Cybersecurity Engagement Leading to First-Cycle FDA Clearance

- Engaged Blue Goat Cyber 6 months before submission target
- Integrated cybersecurity into requirements & design from project inception
- Developed complete threat model, SBOM, and cybersecurity risk assessment
- Achieved first-cycle FDA clearance with no cybersecurity deficiencies

Cybersecurity-First Approach = Regulatory Speed and Market Success

- Secure-by-design principles reduce FDA review cycles
- Complete cybersecurity documentation (18 artifacts) minimizes deficiency letters and RTAs
- Early cybersecurity integration preserves device features and market value

Cybersecurity Maturity is Now a Gating Item for Major Investments

- Investors assess cybersecurity maturity as regulatory risk mitigation
- Strong cybersecurity programs enhance company valuation and deal speed
- Cybersecurity deficiencies increase time-to-market, burn rate, and funding risk

Cybersecurity needs to be on the product roadmap.

Why This Matters – Cybersecurity as a Market Advantage

🚨 Waiting too long = delays, rework, and lost investment.

❌ FDA rejections add months.

❌ Fixing security late costs 3-5x more.

❌ Investors lose confidence.

💡 The best MedTech companies secure devices early.

✔ Faster approvals.

✔ Stronger investor confidence.

✔ Higher market adoption.

Secure your innovation. Accelerate your clearance. Protect patient lives.

- Experts in FDA CDRH cybersecurity expectations and submission support
- 100% success rate with cybersecurity-focused premarket clearances
- Customized cybersecurity strategies to reduce regulatory risk and accelerate market entry

👉 BlueGoatCyber.com

Schedule a Consult with Us Today

The future of healthcare depends on resilient, secure technology.

Let's secure it together.

BLUE GOAT CYBER

THANK YOU

bluegoatcyber.com