

HB Healthcare Business Review

ISSN 2836-7030

healthcarebusinessreview.com



CHRISTIAN ESPINOSA,
Founder and CEO

TREVOR SLATTERY,
CTO



BLUE GOAT CYBER

BETTER LIVING THROUGH SAFER MEDICAL DEVICES



BLUE GOAT CYBER

BETTER LIVING THROUGH SAFER MEDICAL DEVICES



I want to make sure that these devices, which enhance and save patient lives, stay on the market



As 2021 drew to a close, 51-year-old cybersecurity industry veteran and adventurer Christian Espinosa was the epitome of success and good health. Professionally, he had achieved significant success when he sold his first company, Alpine Security, in 2020. Personally, he maintained a physically demanding and active lifestyle, competing in Ironman triathlons and conquering mountain peaks.

However, everything changed in February 2022 when he developed blood clots in his left leg. This near-disaster was narrowly averted with a timely diagnosis, transforming what could have been tragedy into a pivotal moment. What first appeared as sheer luck soon revealed itself as a deeper calling.

Rewind to 2014: Alpine Security was a cybersecurity powerhouse providing solutions across various systems, including medical devices—the very devices that would play a crucial role in saving Espinosa's life years later. Recognizing this as a sign from the universe, Espinosa was inspired to focus on securing these life-saving devices from cyber vulnerabilities. This led to the creation of Blue Goat Cyber, a company dedicated to medical device cybersecurity.

“I want to make sure that these devices, which enhance and save patient lives, stay on the market,” says Espinosa, founder and CEO of Blue Goat Cyber.

UNIQUE NEEDS OF A CRITICAL SECTOR

The challenges in medical device cybersecurity go beyond traditional data theft concerns and pose direct threats to patient safety. Unlike conventional cybersecurity, where the risks center on

unauthorized disclosure of sensitive information, vulnerabilities in medical devices can have life-threatening consequences. Implantable devices like defibrillators could be remotely manipulated to deliver fatal shocks, while diagnostic systems might produce inaccurate readings, leading to untreated and potentially fatal conditions. Even devices like med spa lasers can be maliciously manipulated to cause severe harm, such as burns from intensified lasers with disabled cooling mechanisms.

These risks highlight the need for robust cybersecurity measures tailored to medical devices. The stakes extend beyond safeguarding information to preventing harm, misdiagnosis, and fatalities. Compounding this is the complexity of regulatory compliance, such as FDA and EU MDR clearances, which require meticulous documentation, risk management, testing, and software analysis. Ensuring that innovative healthcare solutions reach the market securely demands expertise and precise processes.

The rapidly evolving healthcare technology landscape, exemplified by innovations like powdered blood for battlefield use, further emphasizes the need for rigorous security evaluations to address emerging vulnerabilities. Striking a balance between fostering innovation and ensuring patient safety, while navigating intricate regulatory frameworks, remains a critical challenge.

SOLUTIONS THAT DELIVER BETTER DEVICES

Blue Goat Cyber meets industry demands by providing comprehensive, tailored cybersecurity solutions that align with regulatory requirements



MELISSA ESPINOSA,
Vice President of
Strategic Partnerships

CHRISTIAN ESPINOSA,
Founder and CEO



while safeguarding patient safety. Their expertise spans devices ranging from med spa lasers to advanced surgical robots, all of which must meet stringent FDA approval standards.

“We have a very rigorous process that we've refined over 10 years to make sure that we're very accurate and complete with all of our medical device cybersecurity assessments,” says Espinosa.

Acting as a third-party cybersecurity partner, Blue Goat Cyber performs thorough testing, identifies vulnerabilities, and ensures devices are secure. The company also advocates for early engagement by integrating cybersecurity into the design phase of product development, helping manufacturers embed security from the outset. This proactive approach minimizes rework, reduces costs, and facilitates smoother regulatory submissions, accelerating time-to-market for innovative devices.

Blue Goat Cyber also distinguishes itself with its fixed-fee model and comprehensive approach to medical device cybersecurity. The company offers flexible services tailored to the unique needs of manufacturers, ranging from complete, end-to-end cybersecurity support—including documentation, testing, and compliance—to targeted solutions such as individual testing. With a fixed-fee structure, Blue Goat Cyber ensures transparency and eliminates the risk of unexpected costs, even if multiple retests are required. Furthermore, the company guarantees its work, addressing any deficiencies flagged by regulatory bodies such as the FDA or EU MDR at no additional cost.

With deep expertise and a flawless track record, Blue Goat Cyber ensures regulatory compliance while helping bring groundbreaking medical innovations to market efficiently

and securely. Their proven expertise and cost predictability make them a trusted and caring partner for medical device manufacturers worldwide.

HELPING CLIENTS, EVERY STEP OF THE WAY

The educational component in medical device cybersecurity is a crucial part of what helps companies go to market more successfully. Blue Goat Cyber follows a structured and collaborative process tailored to each client's unique situation. The process begins with a kickoff meeting to establish clear expectations and assess the client's current level of awareness and readiness regarding medical device cybersecurity. From there, the team identifies the need for targeted discussions with key stakeholders. This often includes separate meetings with the leadership team to align on strategic goals, the engineering team to address technical requirements, and the regulatory team to ensure compliance perspectives are unified.



One of the trickiest parts of the process is harmonizing these diverse perspectives. Management, engineering, and regulatory teams often see cybersecurity through entirely different lenses, which can lead to misalignment. Blue Goat Cyber excels at bridging these gaps by fostering a shared understanding rooted in regulatory standards like those from the FDA or international counterparts. By aligning everyone on the same page, they ensure teams work seamlessly together toward a secure, compliant, and successful submission.

The importance of this aspect is perhaps best described by one of their most recent client engagements. Blue Goat Cyber worked with a large medical device manufacturer, employing around 7,000 people, that had not made a regulatory submission since the previous year, despite having a suite of products. The challenge arose when the FDA issued updated guidance in September, tightening cybersecurity requirements for medical devices. The manufacturer's internal regulatory affairs department recognized that their traditional IT cybersecurity team lacked the specialized expertise required



for medical device cybersecurity. Initially, the IT cybersecurity team was hesitant to collaborate with Blue Goat Cyber, believing that 'cybersecurity is cybersecurity.' This created a need for education and alignment, as the IT team was already frustrated by the regulatory affairs department's lack of confidence in their ability to handle the company's medical device cybersecurity. Blue Goat Cyber stepped in to bridge the gap, providing the specialized guidance needed to meet the new regulatory standards.

This project proved particularly challenging because traditional cybersecurity principles do not align with the unique demands of medical devices. Blue Goat Cyber had to educate the client on the fundamental differences between standard cybersecurity practices and those specific to medical devices, especially regarding how risks are assessed and mitigated by the FDA. The goal was to ensure that any risks were sufficiently addressed to prevent potential harm to patient safety.

Despite the internal bureaucracy and significant educational effort required, Blue Goat Cyber successfully guided the manufacturer through the submission process. The experience highlighted the importance of client education, as traditional cybersecurity professionals often struggle to apply conventional frameworks and methodologies to the specialized field of medical device cybersecurity.

A MISSION TO CREATE BETTER MEDICAL DEVICES FOR THOSE IN NEED

Blue Goat Cyber's strength lies in over a decade of dedicated experience in medical device cybersecurity, beginning with their first company in 2014. This extensive background has enabled them to develop a deep understanding of the unique challenges posed by medical device cybersecurity, setting them apart from traditional cybersecurity firms. Many companies offering traditional cybersecurity services attempt

to extend their expertise to medical devices but often lack the specialized knowledge needed. Blue Goat Cyber's unwavering focus on medical device cybersecurity ensures they understand the specific needs of the industry, including the requirements of regulatory bodies like the FDA. Their expertise allows them to accurately assess devices, evaluate risks, and provide the necessary insights to navigate complex compliance demands.



We have a very rigorous process that we've refined over 10 years to ensure that we are very accurate and complete with all of our medical device cybersecurity assessments

The company is driven by a commitment to ensuring the safe and secure introduction of innovative medical devices to market. Whether working with startups or large corporations, Blue Goat Cyber's mission is to help bring devices that have the potential to improve people's lives to market safely. They recognize that many of these devices, including implantables and surgical robots, incorporate software that can be vulnerable to cyber-attacks, posing significant risks to patient safety. Blue Goat Cyber uses its cybersecurity expertise to secure devices before they hit the market and protect them once in use, ensuring the safety and well-being of patients who rely on them.

Today, Blue Goat Cyber is positioning itself to become a market leader in medical device cybersecurity, with a clear strategy to establish a strong presence in the industry by 2025. After solidifying their foothold in this sector, they plan to expand into robotics, leveraging their existing experience with surgical robots. This extension is expected to take place in late 2025 or 2026, once they have fully established their expertise in the medical device cybersecurity space.

In addition to their focus on growth, Blue Goat Cyber continues to refine their rigorous, ten-year-tested process for ensuring accuracy and completeness in medical device cybersecurity assessments. Looking ahead, they are also developing an AI engine to further enhance efficiency and improve risk management for their clients, adding another differentiator to their already impressive portfolio. With these initiatives in place, Blue Goat Cyber is poised for continued success and expansion in the years to come. **HB**