DEVICETALKS
WEST

Cracking the Code: Insider Cybersecurity Insights for Medical Device Premarket Success

SUMMARY

PRESENTER: Christian Espinosa, Founder and CEO, Blue Goat Cyber

BLUE GOAT
CYBER

Overview

As the medical device industry becomes increasingly connected, robust cybersecurity is critical for market approval and patient safety. After submitting a 510(k) or Premarket Approval (PMA) to the FDA, many medical device manufacturers receive deficiency responses related to cybersecurity. Unfortunately, relying on in-house software developers to address cybersecurity issues is usually a recipe for failure.

Medical device cybersecurity professionals look at the world through a different lens. They are skilled at breaking products and making them work in unintended ways. Turning to a traditional cybersecurity firm is also not recommended for medical device manufacturers. Those companies focus heavily on information disclosure risks, while medical device cybersecurity specialists focus on what matters most—product integrity and denial of service vulnerabilities.

Context

Christian Espinosa discussed unique and pressing cybersecurity challenges facing medical device manufacturers and offered a roadmap for navigating the regulatory landscape and successfully launching products.

Key Takeaways

As medical device connectivity increases, cybersecurity vulnerabilities and patient safety risks grow.

The connectivity of most medical devices is growing through methods like Wi-Fi, Bluetooth, near field communication (NFC), radio frequency identification (RFID), and others.

Research suggests that by 2025, about **70% of medical devices will be interconnected in some way**. As the number of device connections increases, the number of entry points for attackers also grows.

Ransomware attacks are also on the rise. Hospital IT environments aren't very secure. If a hospital environment is compromised, then the medical devices in that facility may be at risk. The consequences for patients can be dire. For example, an in vitro diagnostic (IVD) device may no longer be able to analyze a person's tissue or blood sample.

Cybersecurity vulnerabilities in devices like insulin pumps, pacemakers, and defibrillators are another significant concern for patient safety. Medtronic recently recalled an insulin pump after it was discovered that attackers could remotely connect to the device and alter the insulin delivery. Similar problems have been discovered with cardiac devices such as pacemakers and defibrillators.

To conform with FDA cybersecurity requirements, medical device manufacturers must avoid common pitfalls.

In September 2023, the FDA significantly increased the cybersecurity requirements for medical devices. The FDA now mandates that manufacturers provide a threat model, software bill of materials (SBOM), secure product development framework, and post-market monitoring.

The stronger emphasis on cybersecurity due diligence and risk assessment has caught many manufacturers off guard. Blue Goat Cyber has worked with hundreds of companies to help get their medical devices cleared through the FDA from a cybersecurity perspective.

© 2024 WTWH Media Group.

Based on this experience, Christian Espinosa shared that the top five reasons the FDA rejects medical device company submissions are missing or inadequate:

1. **Threat modeling.** Many organizations don't understand threat modeling and skip it completely. Threat modeling identifies vulnerabilities associated with entry points into a medical device or system.

   The FDA expects manufacturers to evaluate cybersecurity threats using the STRIDE framework. STRIDE identifies whether a threat can cause:

   - **S**poofing
   - **T**ampering
   - **R**epudiation
   - **I**nformation disclosure
   - **D**enial of service
   - **E**levation of privilege

2. **Software bill of materials (SBOM).** The FDA wants to know the lineage of all code used in a medical device. If open-source code is used, for example, manufacturers must determine whether that code has vulnerabilities and what the associated risks are. An SBOM increases the traceability and transparency of code used in medical devices, without divulging a company's intellectual property.

3. **Patient safety-focused risk methodology.** The FDA recommends that medical device companies use risk methodologies focused on exploitability and patient safety. Most cybersecurity risk methodologies focus on information disclosure, which is secondary to product integrity and patient harm.

   Many FDA submissions are rejected because companies evaluate risk using subjective measures, like probability and likelihood. The FDA prefers medical device manufacturers to use a more objective measure like exploitability. The Common Vulnerability Scoring System (CVSS) is a useful tool for measuring the exploitability of cybersecurity threats.

Figure 1: Threat Modeling Diagram Example

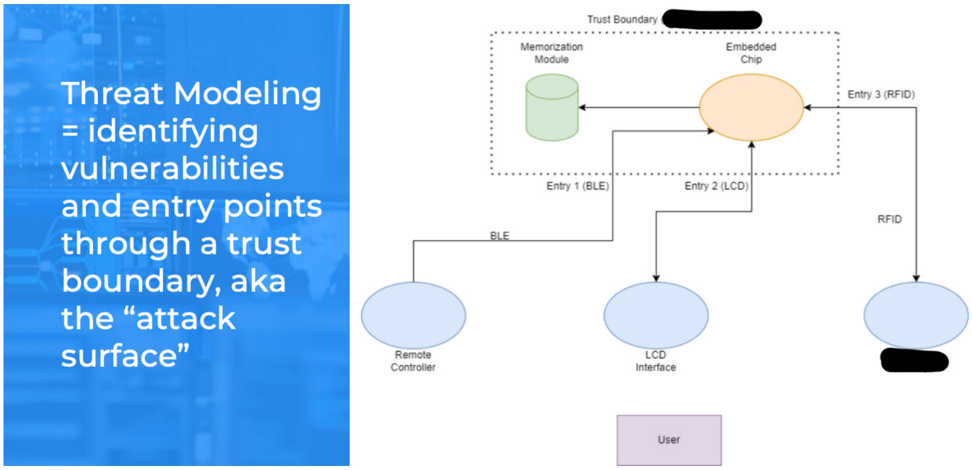
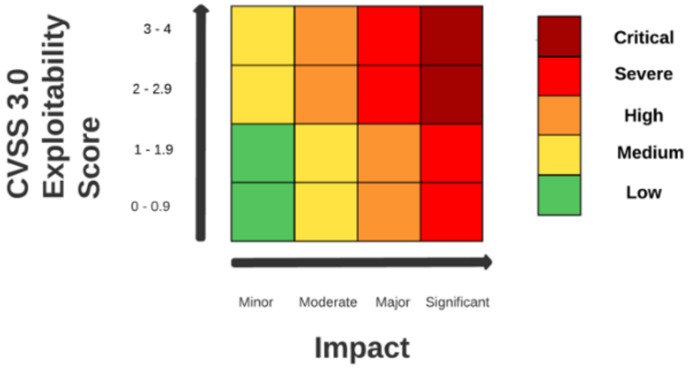

Threat Modeling = identifying vulnerabilities and entry points through a trust boundary, aka the "attack surface"
Trust Boundary [redacted]
Memorization Module
Embedded Chip
Entry 3 (RFID)
Entry 1 (BLE)
Entry 2 (LCD)
BLE
RFID
Remote Controller
LCD Interface
[redacted]
User

Figure 2: Example Risk Matrix



© 2024 WTWH Media Group.

4. **Inclusion of cybersecurity in early design phases.** Designing cybersecurity into a product from the start is much more secure than bolting on cybersecurity at the end of the product development cycle. Waiting to evaluate cybersecurity can also negatively impact a medical device's competitiveness and increase development costs.

   Blue Goat Cyber recently worked with a manufacturer that decided early in product design to use a microcontroller that did not support Secure Boot for code integrity. When the FDA rejected its submission, the company decided to disable the device's cellular and cloud functionality. The resulting standalone device can't gather analytics or monitor patients remotely.

5. **Third-party penetration testing.** During penetration testing, "white hat" cybersecurity teams attempt to break into a medical device using the same tactics as cyberattackers. Unlike vulnerability testing, which only identifies risks, penetration testing exploits vulnerabilities and goes one step further to see how far a bad actor could get into an organization's IT infrastructure or medical device.

   Many manufacturers skip third-party penetration testing and instead try to handle this internally. The FDA, however, requires that an independent third party conduct medical device penetration testing. When selecting a penetration testing company, it's essential to select a firm that specializes in medical devices and to engage them early and often during the product development cycle.

> "Start considering cybersecurity today for your medical devices, even if you're in the design or prototyping phase. That will help you get your device cleared much faster by the FDA."
>
> – Chrisian Espinosa, Blue Goat Cyber

Not all cybersecurity companies are created equal—medical device cybersecurity specialists understand FDA requirements.

Traditional cybersecurity companies are primarily concerned with information disclosure risks. With medical devices, however, these concerns are secondary to integrity or denial of service.

For medical devices, the FDA expects to see a test plan, test cases, and test report. Manufacturers must conduct iterative testing to ensure that problems are fixed, and a medical device's cybersecurity risk is reduced to an acceptable level. These are activities that are familiar to medical device cybersecurity companies. They are not typically addressed by traditional cybersecurity firms.

Cybersecurity best practices are a proven way to get medical devices to market faster.

Four cybersecurity best practices for medical device manufacturers are:

1. **Incorporate cybersecurity in every phase of the medical device lifecycle.** It's essential to incorporate cybersecurity in the early design phases. Manufacturers must also provide a secure way to dispose of medical devices, so protected health information (PHI) isn't leaked.
2. **Be transparent about cybersecurity.** An SBOM can help with this. Consumers have a right to know about third-party software in medical devices.
3. **Focus on patient safety.** Medical device companies must use a risk methodology that aligns with patient safety.
4. **Validate cybersecurity with a third party.** This is a continuous process. Attackers are constantly looking for new ways to break into systems.

> "Once a medical device is cleared by the FDA, that's not good enough. When it's fielded, we also have to monitor for new vulnerabilities because new exploits are constantly evolving."
>
> – Christian Espinosa, Blue Goat Cyber

© 2024 WTWH Media Group.

Other Important Points

- **DevSecOps.** To maximize the cybersecurity of medical devices, developers must work in conjunction with operations and security teams on product development. This approach is called DevSecOps. OWASP offers a playbook for DevSecOps software development practices.

Additional Information

To learn more, visit Blue Goat Cyber

Biography

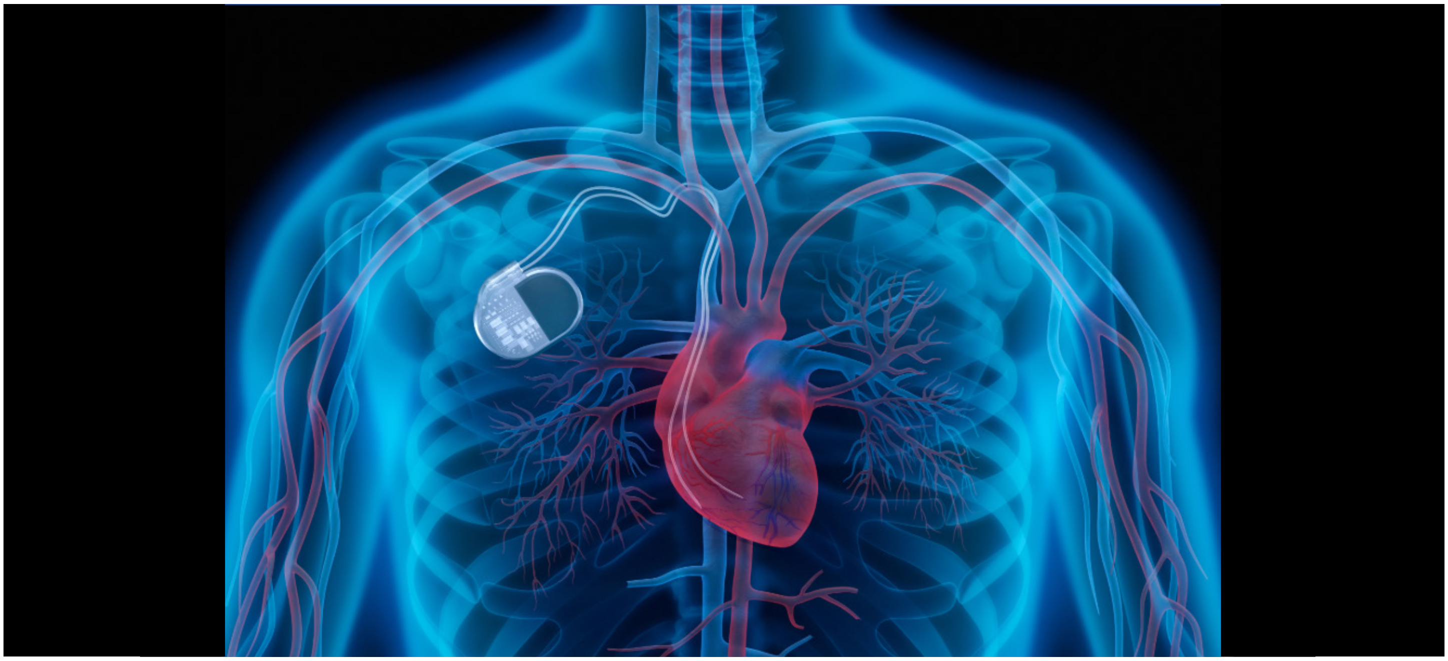
Christian Espinosa

Founder and CEO, Blue Goat Cyber

Christian Espinosa, founder and CEO of Blue Goat Cyber, stands at the forefront of medical device cybersecurity with a mission driven by a passion for problem-solving and a commitment to impactful change. His career path led him to write “The Smartest Person in the Room” and “The In-Between: Life in the Micro,” sharing his evolution from competitive to compassionate leadership.

A pivotal moment in Christian’s life occurred in 2022 when he survived a near-death experience due to six blood clots. The secure medical technology that diagnosed his condition in time saved his life, highlighting the crucial role of cybersecurity in healthcare. This personal health scare solidified Christian’s dedication to ensuring that medical devices are secure and reliable.

Beyond his professional endeavors, Christian is an avid adventurer. He’s a certified skydiver, PADI divemaster, and Ironman triathlete. These achievements reflect his commitment to personal growth and a fearless approach to life. Christian’s down-to-earth personality, combined with his dedication to making a difference, fosters trust and connection. His experiences and insights inspire others to prioritize cybersecurity in healthcare, ensuring medical devices can continue to save lives without compromising on security.



DEVICETALKS WEST

© 2024 WTWH Media Group.