The Cybersecurity Sword Hanging Over Medical Device Manufacturers

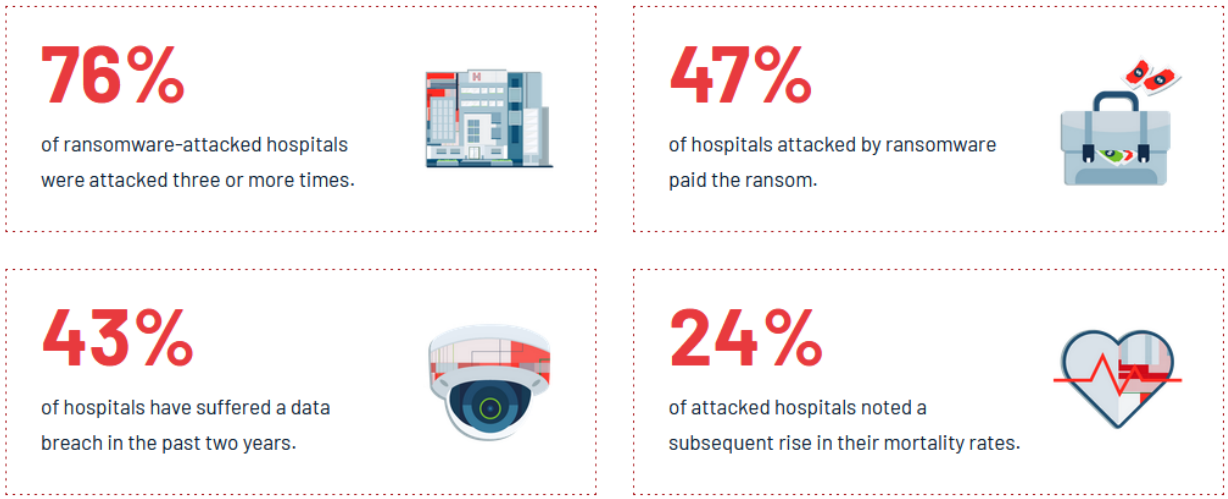

Figure 1: The state of medical device cybersecurity in 2022. Source: Cynerio and The Ponemon Institute, https://www.cynerio.com/ponemon-survey-insecurity-of-connected-devices-in-healthcare-2022

Introduction

In September 2023, the U.S. Food and Drug Administration (FDA) issued a pivotal guidance document titled *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*. This guidance aims to bolster the cybersecurity of medical devices, thus safeguarding patients, healthcare facilities, and the broader healthcare ecosystem from cyber threats. The new regulations require substantial changes in Design Control and Quality Management practices for medical device and in vitro diagnostic (IVD) manufacturers.

This blog post will explore the implications of this guidance, drawing insights from the FDA guidance and the Ponemon Institute's 2022 report, *The Insecurity of Connected Devices in Healthcare*. We will also discuss the types of litigation likely to arise from these new regulations and the qualifications necessary for an expert witness in this domain.

FDA's Cybersecurity Guidance for Medical Device Manufacturers

The FDA's guidance document is not merely a suggestion; it establishes concrete cybersecurity expectations for medical device manufacturers. The guidance emphasizes a proactive, lifecycle approach to cybersecurity, integrating security considerations from the initial design phase through the device's entire lifespan.

Here are some key takeaways for legal professionals involved in this field:

- **Broad Scope:** The guidance applies to a wide range of medical devices, encompassing those with software that stores, transfers, or analyzes data. This includes devices with upgradeable software, USB ports, and even those using compact disc technology.
- **Secure Product Development Framework (SPDF):** The FDA strongly recommends adopting a SPDF, such as the NIST Cybersecurity Framework, to systematically address cybersecurity risks throughout the device lifecycle.
- **Transparency and Documentation:** Manufacturers must provide detailed documentation of their cybersecurity risk management processes, including threat modeling, risk assessment, and security testing results.
- **Labeling and Cybersecurity Management Plans:** The guidance includes recommendations for labeling devices with cybersecurity risks and providing cybersecurity management plans to users.

The Ponemon Report: A Wake-Up Call for the Industry

The Ponemon Institute's report highlights the alarming state of cybersecurity in the healthcare industry. Its findings include:

1. **Widespread vulnerabilities**: 53% of respondents reported that their organizations had experienced a data breach involving a connected medical device. Many connected medical devices are vulnerable to cyber threats due to outdated software, lack of encryption, and insufficient security controls. The report underscores the urgent need for manufacturers to address these vulnerabilities.
2. **Impact on Patient Care:** Cyber-attacks can have dire consequences for patient care, including delayed treatments, compromised data integrity, and increased risk of medical errors. The report calls for a concerted effort to enhance the cybersecurity of medical devices to protect patient safety.
3. **Lack of preparedness**: Only 22% of respondents believed their organizations were ready to respond to a cyber-attack on a connected medical device.

4. **Insufficient resources**: 61% of respondents cited a lack of resources as a significant challenge in securing connected medical devices.

Litigation implications

The new FDA guidance is likely to spur various types of litigation, including:

1. **Product Liability Claims:** Manufacturers may face lawsuits if their devices are found to be inadequately protected against cyber threats, leading to patient harm or data breaches.
2. **Regulatory Compliance Disputes:** Companies may be subject to legal action if they fail to meet the new FDA requirements, resulting in penalties or product recalls.
3. **Intellectual Property Conflicts:** As manufacturers develop new cybersecurity technologies, disputes over patents and proprietary methods may arise.
4. **Contractual Disputes:** Healthcare providers may seek legal recourse if device manufacturers fail to meet contractual obligations related to cybersecurity.

Recent cybersecurity cases have involved prominent medical device companies such as St. Jude Medical[1] and Livanova[2].

What kind of expert witness do you need in these cases?

As litigation related to medical device cybersecurity goes up, securing a highly qualified expert witness will be important. When evaluating potential experts, attorneys should consider the following:

- **Technical skill:** The expert should have deep technical knowledge of medical device software, cybersecurity principles, and industry best practices. Look for certifications like CISSP or CISM.
- **Regulatory knowledge:** A strong understanding of FDA regulations, guidance documents, and international standards related to medical device cybersecurity is essential.
- **Litigation Experience:** Prior experience as an expert witness in similar cases, particularly those involving medical devices and cybersecurity, is highly valuable.
- **Communication Skills:** The expert must be able to effectively communicate complex technical concepts to non-technical finders of fact.

[1] St. Jude Medical, LLC v. Muddy Waters LLC, No. 0:16-cv-03002 (D. Minn. 2016).
[2] J.W. v. Livanova USA, Inc., No. 4:24-cv-02250 (S.D. Tex. 2024).