INSIGHTS

into **MedTech Innovation**

MEDACUITY

MEETING THE CYBERSECURITY CHALLENGES OF TODAY'S HEALTHCARE ECOSYSTEM

Effective Strategies for OEMs

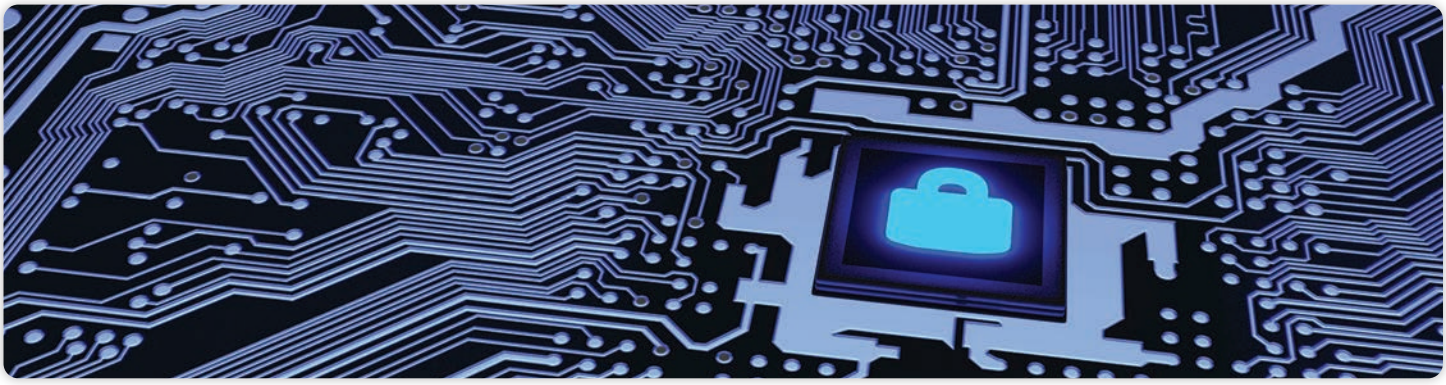
The responsibility to prevent exploitation of cloud-based systems, mobile and wearable devices, Internet of Medical Things (IoMT) products, and legacy devices, as well as those facing obsolescence, fall primarily on the OEM.

Today, healthcare facilities are putting much more scrutiny on medical device OEMs to demonstrate a good understanding of their organization's security requirements and how their solutions can address or alleviate security concerns long before cyber attacks or data breaches arise. According to the FDA, it is the responsibility of the medical device manufacturers (MDMs) to be vigilant in "identifying risks and hazards associated with their medical devices, including risks related to cybersecurity."[1] Although the MedTech industry has a general awareness of the threats, and implications thereof, there is still more that can be done to mitigate the risks.

Challenges Facing OEMs Today

AN INCREASINGLY COMPLEX HEALTHCARE LANDSCAPE

Today's healthcare ecosystem is more complex and distributed than ever before with no signs of abating. Security vulnerabilities and points of entry continue to increase with the proliferation of digital healthcare, wearable and connected devices, patient portals, widespread adoption of BYOD (bring your own device) among caregivers, and more fully integrated technologies of accountable care organizations (ACOs), health information exchanges (HIEs), and payers. Recently, cybercriminals have been exploiting the strain COVID has placed on the overburdened healthcare system. According to findings from Check Point Software, healthcare organizations have seen a 45 percent increase in cyber attacks between November 2020 and January 2021—more than double that of other industry sectors. While ransomware has been the main form of attack, botnets, remote code execution, and DDoS have also been used.[2]



MTINS02-10.2021

CYBERSECURITY UNDERSTANDING AND ACCOUNTABILITY

Organizations grapple with the impact cybersecurity poses. It is no longer a specter. Cybersecurity is real, and front and center, but OEMs face daunting questions about how to adapt their organizations and get ready to address the threat.

- Where do you start?
- Which business functions are most impacted?
- Do we have the appropriate personnel to pull this off?

Additionally, for those organizations who believe they have a handle on it, many still view cybersecurity as something that can be bolted on late in the product development process. But for MDMs to truly succeed, cybersecurity needs to become a lever for holistic organizational change. The importance of good cyber hygiene practices that both complement and reinforce safety risk management within their product development lifecycle must be a priority.

LEGACY DEVICES

While it is true newer devices tend to use wireless communications more often, **legacy medical devices can be even more vulnerable to cyber threats** based on their longevity and technical obsolescence risk. Many legacy devices currently in use in healthcare environments were developed and manufactured well before cybersecurity was a significant concern and are now highly vulnerable. As software systems inevitably become outdated, the risk of being hacked or compromised increases exponentially, putting a patient's personal data and physical safety at heightened risk. This risk also impacts healthcare providers and medical device OEMs in the form of significant reputational damage and financial consequences as a result.

Yet the costs and efforts to update legacy devices to make them cyber-compliant are often prohibitive for OEMs. Some of the struggles they face relate to:

- Swapping out hardware during a refurbish as it goes end-of-life;
- The typical two-year lifespan of software (including Windows) requires timely security patches;
- The five-year sales cycle of some medical devices leaves them quickly unsupportable.

Hospitals and device makers have been at odds as to who bears the burden of making legacy devices more secure. The American Hospital Association has asserted that some basic measures, such as upgrading a device from Windows 7 to Windows 10, should be anticipated by device manufacturers and be a part of expected and affordable maintenance.[3]

OEM Strategies

TAKING A HOLISTIC APPROACH

For a holistic cybersecurity strategy to become truly embedded in an organization, it is critical the overarching approach to developing the program embraces **three pillars** to maximize effectiveness. This year, the FDA debuted draft guidance entitled, "Remanufacturing of Medical Devices" to help clarify at what point changes to a medical device become "remanufacturing" as opposed to "servicing".[4] This draft guidance includes recommendations to help ensure the continued quality, safety, and effectiveness of devices intended to be serviced over their useful life.[5] The following strategies build upon the core tenets and guidance provided by the FDA.

Building out a holistic cyber strategy with FDA-aligned cyber procedures and artifacts is necessary to address the increased FDA scrutiny while getting products out to market. MDM organizations that build out a strong team and process are best suited to select technologies that maximize ROI by making cyber management more efficient in both pre- and post-market scenarios.

TOP DOWN

It is essential for MDMs to stay abreast of rapidly evolving cyber threats and best practices for assessing and mitigating vulnerabilities. From an organizational perspective, the **best place to start with a cybersecurity strategy is at the top**—with C-level executives. It can no longer just be a pain point for product development teams. Further, cybersecurity is not something that can simply be bolted onto a medical device as an afterthought. Turning a blind eye or trying to cut corners will only extend the cost and duration of the development lifecycle. In the worst case, a product with vulnerabilities reaches the market and compromises patient safety or the environment in which it operates.

RIGHT PEOPLE

Teams should be built with the **right people from the appropriate functional areas** of the business who will drive the mission to foster a cybersecurity mindset. For example, the implementers—software engineers—(whether internal or external) must have the qualifications, capabilities, and directive to prioritize security, with a continuously evolving knowledge of the risks and mitigations, and a vigilance for closing gaps.

RIGHT PROCESS

Successful organizations build upon an **"organizational readiness mindset"** as a base for instituting effective and pragmatic strategies across the three pillars. Organizations that make a large investment in cybersecurity monitoring and analysis platforms without the necessary people or process disciplines typically find themselves facing a sizable sunk cost. Conversely, organizations that evolve their cybersecurity discipline across the pillars will earn ongoing dividends on the investment.

RIGHT TECHNOLOGY

A solid strategy is to institute programs across people and processes first, then **apply the appropriate technologies as program needs are better understood.** Starting with the right people who understand cybersecurity and then evolving the team through training and experience is the fastest and most effective track for developing a strong discipline. However, a strong cybersecurity team can only go so far without the necessary process support that demonstrates an effective and repeatable mechanism for managing cyber risks.

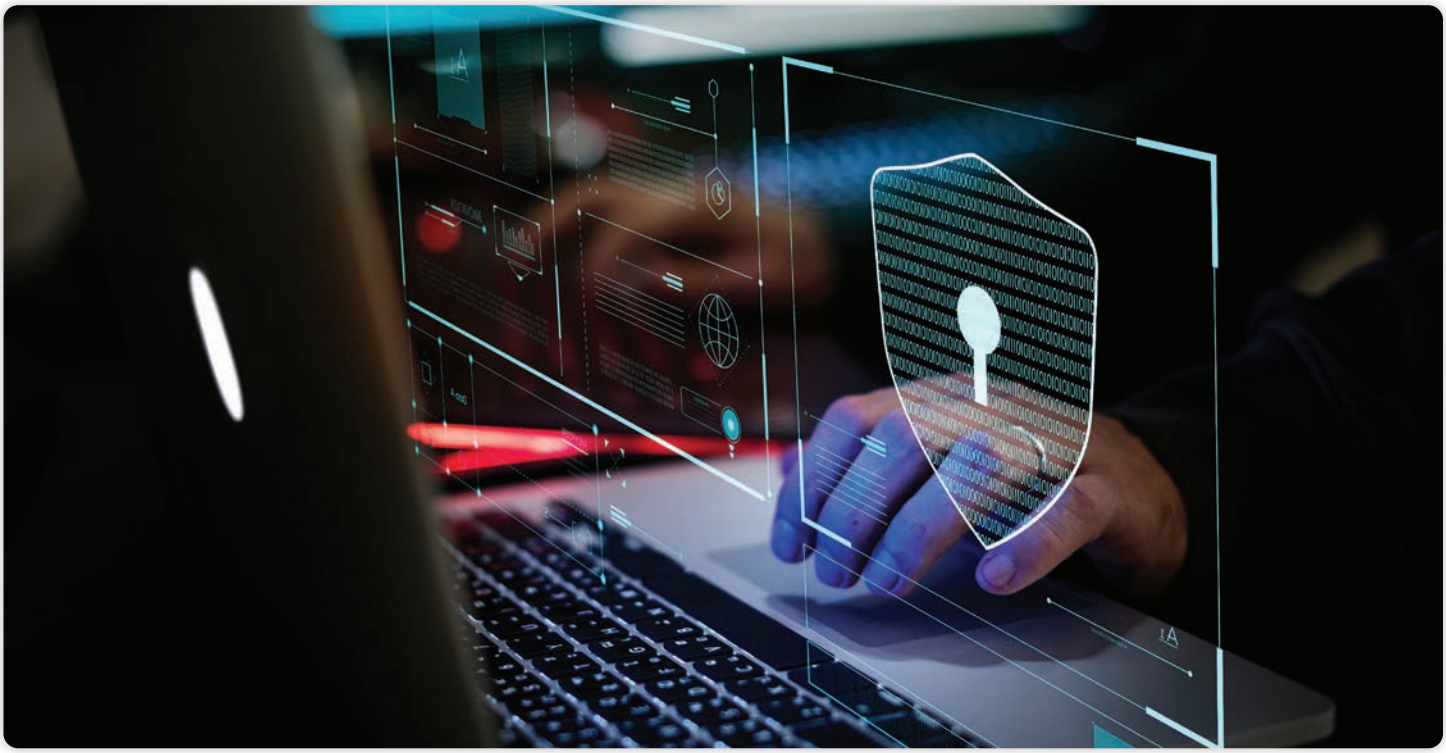
SPECIFIC LEGACY DEVICE STRATEGIES

Anticipating the challenges of legacy devices and **rolling in strategies early on** to mitigate the risks can help prevent significant issues in the long run. Such strategies may include:

- Planned obsolescence—deliver a product to market with a five-year end-of-life plan and with a five-year post-end-of-life support period.
- Select software, such as Windows 10 IoT Enterprise, that has a 10-year lifespan and security support/patch window.
- Refresh product lines more frequently and offer customers upgrade incentives to purge legacy products from the field.
- Lower the cost of ownership or cost of support by managing a device fleet remotely.
- Respond to new vulnerabilities and threats more rapidly with over-the-air updates.

MAKING THE BUSINESS CASE FOR CYBERSECURITY

Investing in cybersecurity early and doing it with a holistic mindset can equate to less money and effort spent on late-stage fixes or damage control when a data breach or cyber attack happens. Overall, this contributes to maximum gross profits by minimizing the likelihood of costly adverse events, and the associated reputational and intellectual property exposure adverse events can create. There are also greater efficiencies gained through optimal FDA compliance. This minimizes the barriers of selling to the end-client healthcare facility, whose IT department rigorously vets a checklist of the cyber considerations of its chosen MDM.



Bottom Line

In 2020, IBM reported a data breach costs a healthcare organization an average of $7.13 million—a 10 percent increase from the 2019 average.[6] Therefore, it's no surprise they are increasing the scrutiny on the OEMs they opt to do business with. For medical device companies to continue adding value to the healthcare ecosystem through transformative solutions without introducing unmitigated risk, cybersecurity can no longer be an afterthought or a bolt-on. Instead, it must be a key consideration valued from the top of an organization down. Best practices need to be baked into every aspect of the product development lifecycle and investments made in the right people, process, and technology along with legacy device strategies to effectively combat cyber risks.

ABOUT THE AUTHOR

Jarman Joerres | *Co-Founder & Principal, MedAcuity*

Jarman is a senior software architect and cybersecurity specialist. He works exclusively with MedTech companies to solve the business and technical challenges inherent in developing complex software-driven medical devices and solutions.

Contact MedAcuity - info@medacuitysoftware.com

REFERENCES

1. *https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity*
2. *Cyberattacks on Healthcare Spike 45% Since November | Threatpost*
3. *Microsoft Word - EC RFI Device Security Letter_5-31-2018_for posting.docx (aha.org)*
4. *"Remanufacturing" or "Servicing"? New FDA guidance clarifies distinct - Hogan Lovells Engage*
5. *FDA In Brief: FDA Issues Draft Guidance on Remanufacturing and Discussion Paper Seeking Feedback on Cybersecurity Servicing of Medical Devices | FDA*
6. *IBM Report: Compromised Employee Accounts Led to Most Expensive Data Breaches Over Past Year - Jul 29, 2020*

ABOUT MEDACUITY

MedAcuity, a specialized engineering firm, develops custom software solutions to address the most critical product development challenges facing MedTech and Robotics companies and innovators. With over a decade of experience in software design and development methodologies for highly regulated and compliance-driven industries, our technical capabilities span all levels of software from embedded systems to mobile devices, the cloud, and enterprise technologies. Our cybersecurity consulting practice continues to evolve to meet the growing demands from clients to develop robust cybersecurity programs that align with FDA requirements.