INSIGHTS

into **MedTech Innovation**

MEDACUITY®

CYBERSECURITY FOR TODAY'S COMPLEX HEALTHCARE ECOSYSTEM

Effective Strategies Start at the Top

The risk of cyber threats to the global healthcare ecosystem is undeniable – and growing.

Hospitals and other point-of-care environments are facing the enormous challenge of providing patients with the most innovative and advanced medical technologies, while also keeping all stakeholders safe from cyber attacks that exploit vulnerabilities in the rising number of cloud-based systems, mobile and wearable devices, and the Internet of Medical Things (IoMT), as well as aging legacy devices and those facing obsolescence.

In response, hospital administrators are starting to take a firm, multidisciplinary approach to develop more comprehensive cybersecurity strategies and include clinicians, IT, and security teams in formal purchasing processes. Healthcare facilities are putting much more scrutiny on medical device OEMs to demonstrate a good understanding of their organizations' security requirements and how their solutions can alleviate security concerns long before cyber attacks or breaches arise.

For medical device companies to continue adding value to the healthcare ecosystem through transformative solutions without introducing unmitigated risk, cybersecurity cannot be an afterthought or a bolt-on. It is essential that accountability and enforcement come from the highest levels of their organizations, and that cybersecurity is a consideration in every aspect of the product development lifecycle.

Today's Healthcare Landscape

For years, hospitals have put significant effort in to carefully controlling and managing their "on-prem" environment. With servers, they knew who was monitoring them and how; what default tools were installed; and how they would someday be decommissioned. By comparison, today's healthcare ecosystem is complex and distributed; comprised of devices, users, suppliers, and extremely sophisticated software systems that expand the network perimeter, each bringing benefits and introducing risks.

Connected devices offer many advantages in terms of allowing healthcare providers to collect, monitor and analyze patient data more quickly and accurately than ever before. While this can facilitate more effective care, improve patient outcomes, and even save lives, hackers have become adept at exploiting device vulnerabilities for malicious purposes. Security vulnerabilities and points of entry continue to increase with the proliferation of wearable devices and 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.

IoMT devices, specifically infusion pumps, implantable devices, and vital sign monitors that make use of wireless technology for the transmission of data and commands, can all be subject to significant security vulnerabilities.[1] These weaknesses may create opportunities for hackers to remotely take control of a medical device to change or impair its function, or to gain access to privileged Personal Health Information (PHI). The stakes are simply too high to consider cybersecurity as anything other than a top organizational priority.

> *“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% increase in cyberattacks 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] ”

While it is true that newer devices tend to use wireless communications more often, legacy devices can be even more vulnerable to cyber threats based on their longevity and technical obsolescence risk. 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.

It is ultimately up to the hospitals to make the best purchasing decisions to support their patients’ needs. However, 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.”[3] Although the MedTech industry has a general awareness of the threats, and implications thereof, not enough of them are taking the proper approach to mitigating the risks.

The Price of Inadequate Cybersecurity

Patient safety and data privacy are of paramount concern with respect to a cyber attack, but the business implications of a PHI breach can also be staggering and long-lasting. Healthcare organizations have the highest costs associated with data breaches, resulting in part from a combination of lost business, lost revenue due to system downtime, and the impact a diminished reputation has on gaining new business.[4]

- In 2020, IBM reported that data breaches cost healthcare organizations **an average of $7.13 million** – a 10% increase from the 2019 average.[5]

- In a growing number of cases, the HHS Office for Civil Rights has imposed financial penalties on covered entities and their business associates that violate HIPAA policies due to data breaches. In the largest settlement to date, **Premera Blue Cross paid $6,850,000** to resolve a case resulting from a 2014 data breach that affected 10.4 million members.[6]

Cybersecurity – Where to Start and Who's Responsible?

There is no silver bullet or one-size-fits-all approach to cybersecurity. You can easily get lost down a rabbit hole when trying to identify an effective approach. For MDMs to 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 the product development lifecycle must be a priority.

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.

Therefore, it is essential for MDMs to stay abreast of rapidly evolving cyber threats and best practices for assessing and mitigating vulnerabilities. Executives at the highest levels must change their thinking on how they approach cybersecurity—making it a business priority with appropriate investments to mitigate both patient and business risk.

> *“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.”*

MedAcuity Perspective: Critical Success Factors to Proactively Attack the Challenge

Working within all levels of MDM organizations provides us with a unique perspective on how companies continually struggle with cybersecurity. In our experience, companies that have successfully mitigated this risk have an executive champion who promotes a strategy built on three main pillars: right people, right process and right technology.

For a holistic cybersecurity strategy to become truly embedded in an organization, it is critical that the overarching approach to developing the program embraces these pillars to maximize effectiveness. Being “organizationally ready” requires more than a mandate or a statement from the executive champion. It requires the champion to be accountable for driving the three pillars.

RIGHT PEOPLE

The executive champion identifies the right people from the appropriate functional areas of the business to build the team who will drive the mission to foster a cybersecurity mindset. In our experience, organizations that just check boxes and don't hold the organizational functions accountable struggle to achieve the cybersecurity discipline required for today's ever-evolving medical device industry.

RIGHT PROCESS

Successful organizations build upon this “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. The majority of organizations that don't follow this approach are sold on the tools as a quick solution, and then realize they either chose the wrong tools or they require considerable investment, knowledge and configuration to make them work correctly if at all.

Additionally, the wrong tools can create costly inefficiencies because the outputs and reporting are not aligned with organizational needs, consequently generating uninterpretable data that provides little if any value. A common refrain we hear is, “I receive this cybersecurity report every month; I can make no sense of it and I don't know what to do with it.” The best strategy is to build a holistic cybersecurity vision that covers IT, R&D, and other similar organizational needs, leverage a cross-functional team who understands the organization (right people and right process), and select a combination of technologies that, when combined, enables you to successfully implement the vision.

Bottom Line

Building a strong and resilient cybersecurity program that holds up to stringent medical standards doesn't happen overnight, but it's crucial for mitigating the ever-increasing patient and business risks that these threats pose. With increased scrutiny from healthcare facilities, medical device OEMs are being put on notice by their customers and the FDA. They need to have their cybersecurity house in order or run the risk of significant business implications in terms of recalls, fines, reduced sales and revenue, and reputational damage.

ABOUT THE AUTHOR

Jarman Joerres | *Cybersecurity Specialist, 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. With a keen focus on clients' business goals and a commitment to security-by-design, he works to ensure the right level of security for each unique development project.

Contact MedAcuity - info@medacuitysoftware.com

SOURCES

1. *IoT News - 4 IoT Medical Devices That Are Vulnerable to Hacks - IoT Business News*
2. *Cyberattacks on Healthcare Spike 45% Since November | Threatpost*
3. *https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity*
4. *Average cost of healthcare data breach rises to $7.1M, according to IBM report | FierceHealthcare*
5. *IBM Report: Compromised Employee Accounts Led to Most Expensive Data Breaches Over Past Year - Jul 29, 2020*
6. *September 2020 Healthcare Data Breach Report: 9.7 Million Records Compromised (hipaajournal.com)*

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.

MEDACUITY