Medical Device Cyber Trends

Cybersecurity in the medical device industry

This is the first offering in our series on cybersecurity in the medical device industry. Stay tuned for more on emerging trends, opportunities and challenges. Or, for more information, contact a member of our life sciences cybersecurity services team.

In the quest for medical device innovation, don't forget cybersecurity

In today's changing medical device landscape, with current guidelines and developing regulations, understanding technical requirements impacting the medical device industry is only part of the equation. Similar to other industries, medical device manufacturers must detect signals of change and capitalize on disruptors before their products become obsolete. They must also be attuned to marketplace accelerators that could propel their products to new levels. An often-neglected aspect of the quest for innovation is the need for a multi-year cybersecurity and technical risk plan. Such a plan must align with organizations' business goals and objectives, as well as their strategic direction.

In an industry where healthcare and life science solutions are driven by more than just technology innovations, medical device organizations' success depends on properly investing, as well as understanding both current and future trends. The most successful organizations will be able to adapt quickly, taking advantage of industry trends to meet both patient demand and patient needs. It is critical to stay at least one step ahead of market disruptors and accelerators, such as technology-based innovations like sensor-based wireless devices and 3D printing; clinical developments like Next Generation Sequencing (NGS); demographic shifts like the aging of Baby Boomers; and regulatory change, such as evolving reimbursement guidelines.

Above it all, the most successful companies will view all strategic decisions through the lens of cybersecurity considerations and evolve their businesses so that cybersecurity readiness becomes a competitive differentiator.

Sensor-Based Wireless Mobile Medical Devices are both an Opportunity and a Challenge

Rapid developments in wireless technologies and sensor-based wireless devices have ushered in a new era of mobile medical devices. These devices are improving patient quality-of-life and lowering costs for both healthcare providers and

patients. Mobile medical devices come with significant advantages, given their more compact size and networked capabilities. For patients this means fewer trips to the hospital and greater freedom of movement. For providers, this means dramatically reduced administrative overhead and cost of providing care. Considered a form of telemedicine when applied to healthcare, the overall wearable market is expected to grow from $20B in 2015 to almost $70B in 2025, according to the National Institutes of Health.

Despite the significant advantages and conveniences, mobile medical devices come with new security and technical risks. For example, a typical sensor-based mobile medical device will have a low-power wireless communications system, such as a Bluetooth Low Energy (BLE) or ZigBee radio. The use of low-power radios requires an intermediate base station in close proximity to the user (e.g., 150 meters maximum for BLE) so that data can be transmitted and subsequently uploaded to a "secure" server through a wireless network.

---

1. *Pradeeep Kumar and Joon-Hae Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey," US National Library of Medicine, National Institutes of Health (2012): v12 (1), accessed January 5, 2017*
2. *"Novel Sensing Technologies Prompt Progress in Wireless Medical Devices," accessed January 10, 2017, Qmed website.*

If malicious hackers use a powerful receiver antenna, they may be able to intercept, modify or extract patient data. This poses a serious threat to patient security and privacy.[1] Medical device manufacturers must ensure that they assess their technical environment's product and solutions for known vulnerabilities and remediate any notable findings, promptly. They must also address challenges ranging from power and usability issues, to data transmission in mobile medical devices.

To address security concerns, strong collaboration among medical device manufacturers and sensor and semi-conductor chip suppliers is required. The stakes have never been higher for these groups to forge strong relationships and align on delivering ground-breaking products while ensuring patient safety.[2]

Three-Dimensional (3-D) Printing will Revolutionize Personalized Medicine

Researchers calculate the current value of the 3D printing industry to have reached the $700 million mark already. The 3D industry as a whole is projected to grow to $8.9 billion in the next 10 years, which would represent growth to a 21 percent share of the market. The medical sector is expected to account for $1.9 billion of the total.[3]

While the use of 3D printing technologies in the medical device industry is still in its infancy, this technology could significantly revolutionize how devices are manufactured and cause huge disruption to the industry. Medical applications for 3D printing are expanding exponentially and are expected to impact not only implantable and non-implantable devices, but execution of services and on-demand capabilities.

Medical device manufacturers cannot afford to wait and see how things evolve. They should keep a close watch on developments and start thinking about how they will use 3D printing to foster innovative new products.

On the other hand, since the 3D printing industry is new and evolving, there are no regulatory guidelines related to cybersecurity and privacy. At present, the FDA regulates 3D-printed medical devices just as it regulates any other medical device with the exception of stricter software and material specifications. In the meantime, manufacturers exploring 3D printing need to address the specific kinds of cyber-threats produced by this technology. For example, there is the potential for hackers to tamper with the device during the printing process, altering its efficacy by up to 25 percent, according to a study from New York University's Tandon School of Engineering. Further, if design files contain sensitive patient information, the risk of violating the patient privacy laws is high as well.

Next Generation Sequencing (NGS) will facilitate early detection

The current medical model focuses on the detection and treatment of pathologies. Treating disorders, especially those in advanced stages, is very expensive for patients and society in general. Next Generation Sequencing (NGS) has the potential to accelerate early detection of disorders and to pinpoint pharmacogenomics markers to customize treatments. In regard to the latter, more than 120 currently approved drugs already have pharmacogenomics data in their labeling, thus providing information on variability in patient responses, according to the New England Journal of Medicine.

Early screening for five of the most common disorders in the US (cardiovascular disease, stroke, cancer, chronic obstructive pulmonary disease, and diabetes) could protect millions of lives and reduce the healthcare deficit. Drug therapies are already being tailored to individual patients via personalized medicine (PM), and improvements are being seen in cancer treatment and prevention of adverse drug interactions and fatalities.

The FDA's flexibility[4] in evaluating NGS systems is encouraging developers to move as expeditiously as technology allows. With the focus on precision medicine involving NGS accelerating, medical device organizations would be wise to consider this trend and design therapeutic devices that support NGS to gain a competitive advantage.

Developing NGS technologies requires intensive and frequent collaboration between disparate research facilities. Therefore, manufacturers should bear in mind the increased need for cyber-vigilance when it comes to sharing data and collaborating on research across global sites.

An aging population will drive growth in implants and wireless communication.

Implantable medical devices (IMDs) have a history of outstanding success in the treatment of many diseases, including heart diseases, neurological disorders, and hearing loss. The aging Baby Boomer generation, a population which will reach 88.5 million between 2010 and 2050,[5] represents a tremendous opportunity for growth for medical device manufacturers in terms of market share and new product development.

At the same time, they present challenges not yet experienced by medical device manufacturers. Some of these challenges are: [6]

1. The average life expectancy for a 65-year-old American is 17.7 years for a male and 20.3 years for a female. This is three to four more years of life expectancy than the prior generation had at the same age. This longer life expectancy may lead to increased health concerns and disability in later years, thereby driving demand for newer applications of medical devices.
2. Although Baby Boomers are more active than their predecessors, they are not necessarily the healthier generation. They are more prone to obesity, diabetes, high blood pressure, etc. and are, therefore, more likely to require medical devices.
3. Baby Boomers are early adopters of medical advances such as those seen in orthopedics, implants, and wearable

---

3. *C. Lee Ventola, "Medical Applications for 3D Printing: Current and Projected Uses," P&T (2014): v39 (10), accessed December 14, 2016.*
4. *"FDA Holds Public Workshops to Discuss Regulatory Strategies for Next Generation Sequencing Diagnostics, Part 1," accessed December 15, 2016, Weinberg Group website.*
5. *"The Next Four Decades: The Older Population in the United States: 2010 to 2050," accessed December 12, 2016, Census website.*
6. *"Ageing Population Trends in the Medical Device World," Medical Tracking Solutions Blog.*

technology. At the same time, Baby Boomers demand high-value, low-cost solutions that offer improved quality of life.

Given the prevalence of chronic conditions, the demand for high value and the increased life expectancy of Baby Boomers, medical device manufacturers must be in the position to predict their needs and introduce cost-effective life-changing products as the market demands. Manufacturers can leverage tools and techniques that allow predictive data analysis, such as Data Analytics, Data Science and Data Transformation.

Of course, any use of Big Data comes with concurrent cybersecurity requirements. While the amount of patient data and the tools available to analyze it are at all-time highs, the risk to protected patient information is also higher than ever before. As in all industries, medical device manufacturers must foster industrywide collaboration on standards, technologies and protocols related to the security of customer data.

Reimbursement will rival safety and effectiveness as a development goal.

Reimbursement, as it applies to medical devices, is defined as the payment a third-party, public or private insurer pays a healthcare provider for costs or payments the provider incurred while using a medical device or performing a procedure. If coverage is uncertain, it is difficult for the manufacturer to predict whether an investment in a new technology will provide sufficient returns.

Reimbursement will be a driving factor in securing venture funding for mHealth technologies and medical devices. Under a value-based care model,[7] device manufacturers must not only demonstrate clinical utility, but also quantify the economic benefits associated with producing cost-effective outcomes. This increases pressure in an already risk-averse investor environment.

Whether a device or procedure is reimbursable, and at what amount, can have a significant impact on a provider's ability to access a particular technology, as well as a manufacturer's ability (or willingness) to provide it. Reimbursement is no longer guaranteed simply because a device is superior to existing alternatives. In order to tackle reimbursement challenges and changes,[8] medical device manufacturers must consider the following:

1. First, develop a reimbursement assessment early, while still in the product design phase. It is essential to understand how a particular device may or may not fit within current payment methodologies such as DRGs, resource-based relative value scale (RBRVS), or bundled payments. Find out sooner rather than later about prospects for coding, coverage, and payment – essential variables of reimbursement. Then develop a reimbursement strategy.
2. Second, identifying the clinical problem first. Retrofitting technology from another application with hopes of making it suitable as a covered medical device rarely works.

Cybersecurity capabilities will become competitive differentiators

Throughout all of these developments, it is critical to elevate cybersecurity in medical devices to an organizational imperative, approached with the same rigor as patient safety and quality standards. Patients are demanding this. As per a recent healthcare survey, 50 percent of consumers said they would think twice about using any network-connected medical device, and 62 percent said they value cybersecurity more than ease of use.

Although regulators struggle to ensure devices' safety and efficiency without stifling innovation, recent guidelines by the FDA recommend that manufacturers consider implementing cybersecurity capabilities throughout a product's life cycle.[9] It is important for medical device organizations to take a proactive approach to cybersecurity by considering and implementing measures and capabilities from the initial concept and design phase, throughout each related process, and through to the end of a device's life. Pro-actively implementing cybersecurity throughout an organization will position it ahead of competitors.

While the FDA's cybersecurity guidelines are not currently enforced as regulations, manufacturers must be proactive and develop plans to address the same. Since there is heavy competition for market share among similar product lines, manufacturers that take a proactive approach to address cybersecurity concerns, and position their cybersecurity capabilities as differentiating factors, will emerge as industry leaders and best of breed. This status can only be accomplished by budgeting for and building cybersecurity into the design process, showcasing cybersecurity and leadership abilities in this emerging space, and demonstrating FDA compliance.

[7] *Lisa Weeks, "Reimbursement: A Medical Device Company's Worst Nightmare," Master Control Inc. Blog, August 12, 2015.*
[8] *"Top Reimbursement Tips for Medical Device Makers," MDDI Blog.*
[9] *"Post-market Management of Cybersecurity in Medical Devices," accessed January 3, 2017, FDA website.*

Conclusion:

For the medical device industry as a whole to thrive, each organization must consider its next movements and where to get the most return for its investment dollars. While organizations would be wise to align their investments with their business goals and objectives, they must also keep a keen eye on potential disruptors and accelerators that could significantly transform their businesses. Otherwise, they may wind up like countless other established and well-known companies that were slow to innovate or adapt new technology and rapidly faded away within the market. From disruptive technology trends that increase convenience and accuracy, to patient demand for more technologically advanced and secure devices, manufacturers must closely observe the pulse of the market and determine how to gain distinct advantages. And it is critical to remember that a ground-breaking product is only as good as the security that governs it.

Contact:

Larry Mraz
Director, Advisory,
Medical Device Cybersecurity Lead
T: 973-912-6161
E: lawrencemraz@kpmg.com

David Remick
Partner, Advisory,
Life Science Cybersecurity Lead
T: 404-222-3138
E: jremick@kpmg.com

kpmg.com/socialmedia