ABIresearch®

REPORT

OCTOBER 11, 2016

MEDICAL DEVICE CYBERSECURITY

Michela Menting: Research Director
Jonathan Collins: Research Director

TABLE OF CONTENTS

1. NEW CYBER CHALLENGES

Healthcare is one of the largest industries in the world and expenditure continues to grow significantly. The World Bank calculated US$7.8 trillion spending globally in 2013, up from US$6.5 trillion estimated by the World Health Organization in 2010. Health expenditure is defined by the World Bank as the sum of public and private health spending, covering the provision of health services (preventive and curative), family planning activities, nutrition activities, and emergency aid.

On average, global expenditure on health represents 10% of a country's gross domestic product (GDP). Unsurprisingly, the correlation between wealth and health is relatively tight, with OECD countries closer to the 12% mark. At the highest end of the scale, which is in the United States, health expenditure accounts for 17% of the GDP. It is the country with the highest total spending per person per year (averaging over US$8,000, which is 2.5 times the OECD average, and 8 times the global average). Countries emerging in the developed phase are seeing greater focus on healthcare.

The continued progression of care naturally relies on the development of improved facilities, better instruments, and new drugs for more efficacious treatments and cures. Technology plays a crucial role in advancing healthcare and information and communication technologies drive forward the modernization of the industry. Ultimately, the goal is the provision of more affordable healthcare and universal access.

As with all connected technology adoption, issues are emerging in terms of security. The Internet and its associated enabling technologies bring with it a host of insecurities that are capable of affecting patient safety. The forthcoming challenge for the healthcare industry is to be able to take advantage of technological benefits while minimizing the potential risks that may be incurred. The balance is not an easy one to reach and requires education in new areas, notably cybersecurity. While many of the current fields of research on the topic have focused around data protection, there is an equally important aspect to consider: the protection of medical devices.

An IT health infrastructure will include many of the same pieces as traditional enterprise IT (servers, databases, computers, and smartphones); however, the similarities stop there. The incorporation of connected medical devices into the IT network poses new issues around safety and security, and ultimately presents new and unknown threat vectors around the operational side. The concept of a medical internet of things (IoT) is quickly emerging. Healthcare professionals must consider confidentiality, integrity, and availability mechanisms not just for patient data, but also with respect to medical devices, ensuring that they are protected accordingly.

1.1. METHODOLOGY

This report first analyzes the current risks posed by medical devices, noting various security issues, potential vulnerabilities, and the threat landscape. The following section reviews implementation mechanisms and efforts in medical device cybersecurity and safety. The final section reviews how the healthcare ecosystem is responding to the issue and identifies the vendors driving change.

ABI Research aggregated all available information from research interviews and internal data. Vendor interviews and key assumptions were examined against ABI Research's internal analysis reports and databases, including:

- *IoT Market Tracker - Worldwide*
- *Critical Infrastructure Security*
- *Wireless Healthcare and Fitness*
- *Critical Infrastructure Security: Healthcare*
- *IoT Services for Medical Imaging Equipment Market: MRI, X-ray, CT Scanners, and Tomography*

Some of this information is made publicly available; some is not public, but can be used in aggregate without revealing specific information. ABI Research also used regional and global economic forecasts, and information on recently released annual reports and SEC filings, white papers, standards and specifications, best practices and guidelines (notably National Institute of Standards and Technology (NIST), FDA, and UL), product sheets, industry periodicals, trade group reports, public and private databases, and Internet research to understand the current and future market potential for cybersecurity in medical devices. A number of key assumptions regarding the market size for the different splits, industry verticals, and geographic market shares are made in order to develop an effective forecast model.

1.2. THE MEDICAL INTERNET OF THINGS

Networked devices can improve the tracking, development, sourcing, and distribution of medical technology

Healthcare is increasingly dependent on technology and both the demand and need for connectivity are increasing. Networked devices are improving the manner in which medicine is tracked, developed, sourced, and distributed. In addition, medical technology can offset increasing costs, decrease medical errors, improve patient outcomes, improve access to care, and deliver specialized knowledge to the bedside.

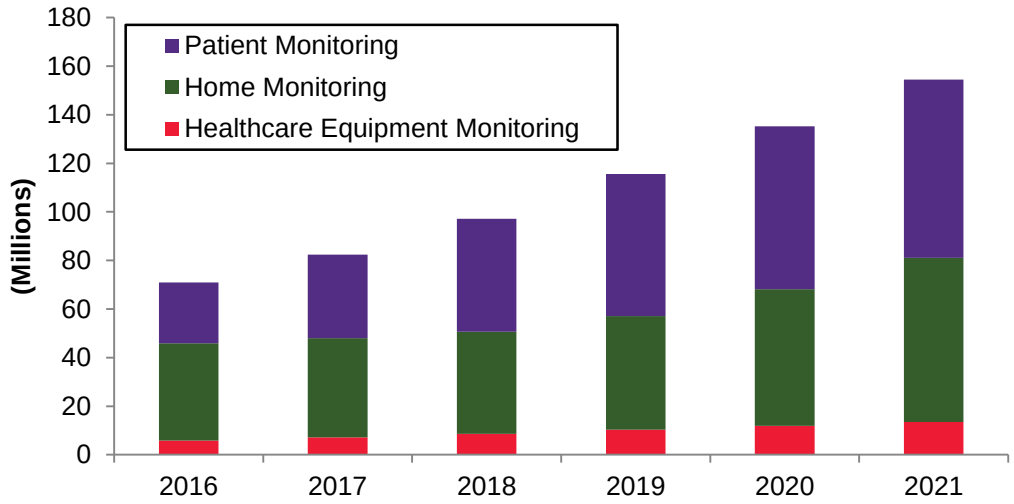
The sheer number and diversity of medical devices available in healthcare is already overwhelming and the medical IoT is going to connect even more devices to the health IT infrastructure. Small, portable devices (pacemakers, continuous glucose monitors, wearable insulin pumps), on-site, mobile appliances (diffusion pumps, bed head units, oxygen appliances), and large, fixed machines such as imaging equipment (X-rays, MRIs, CT scanners) will be connected to back-end servers hosting patient databases and to healthcare applications and front-end interface devices for medical professionals.

ABI Research calculates that there will be 154 million connections for healthcare equipment, home and patient monitoring by 2021 (see Table 1 and Chart 1 below), up from 70 million by the end of 2016. For more information, see ABI Research's *IoT Market Tracker - Worldwide* market data.

Table 1: Health Monitoring Connections
World Markets, Forecast: 2016 to 2021 *(Source: ABI Research)*

Segment	Connections	2016	2017	2018	2019	2020	2021	CAGR 16-21
Healthcare Equipment Monitoring	(Millions)	5.81	7.10	8.65	10.31	11.87	13.55	18.5%
Home Monitoring	(Millions)	40.09	40.90	41.97	46.82	56.25	67.57	11.0%
Patient Monitoring	(Millions)	25.00	34.45	46.57	58.43	67.06	73.37	24.0%
Total	**(Millions)**	**70.90**	**82.44**	**97.19**	**115.57**	**135.19**	**154.49**	**16.9%**

Chart 1: Health Monitoring Connections
World Markets, Forecast: 2016 to 2021 *(Source: ABI Research)*



Healthcare equipment monitoring includes imaging (MRI, X-ray, *etc*.), lab diagnostic, and patient monitoring equipment. Home monitoring designates wearable and wireless-enabled devices, appliances, and gateways used for aging in place, personal emergency response systems (PERS), and ambient assisted living applications. Patient monitoring includes regulated wearable wireless-enabled devices, appliances, and gateways used in doctor-prescribed monitoring applications for remote and on-site professional healthcare use. The connections do not include those for fitness and sports-related monitoring devices.

Connectivity will be enabled through various technologies, including cellular (2G, 3G, and 4G), 802.15.4, Bluetooth, Fixed Line, LPWA, and Wi-Fi. This diverse range will make for a rich, but also increasingly complex medical IoT, where network management will play a key role.

1.3. MANAGEMENT OBSTACLES

The technical challenges involved in the millions of network connections require new ways to avoid risks faced by IT devices

Being able to manage these millions of connections on a network is going to be challenging because, by nature, they can be vastly different from each other and from those used in traditional IT settings. Existing knowledge and experience may not always apply in this new setting. The technical challenges are numerous (management, patching, updating, monitoring, *etc*.) and they cannot always accept the same levels of risk as IT devices (*i.e.*, reboot or downtime, for example).

The various operating systems, network protocols, software, and firmware used, the support of legacy devices with lifespans that last decades, the onboarding of new connected appliances, and the link to electronic health records (EHRs) and health applications all create new challenges. While enabling the interface between EHRs and medical devices means improving quality of care and patient safety through interoperable and data sharing devices, this also creates new risk scenarios, which may jeopardize the goal of better patient care delivery.

For effective management of medical devices, there is the prerequisite of device visibility. This means not just visibility on the network, but also having detailed information about the device itself (features and functions). This is necessary in order to correctly identify devices, scanning and assessing them in terms of risk. Without such information, it is difficult to quantify the likelihood that onboarding a medical device may compromise patient safety or care delivery.

However, information gathering on device functionality is not easily done, often because manufacturers do not always make such information available. It is difficult to build effective security policies and access control measures without in-depth information about devices. As a result, healthcare providers have a hard time building comprehensive inventories of devices in order to manage them accordingly.

Furthermore, many medical devices live in a handoff zone, which adds to the complexity of management. When patients move from one floor to another, or in and out of a healthcare organization, the devices need to transition to other networks. Most sit behind a firewall protecting them from external networks, but are not further managed in terms of protecting them from internal threats. Authentication and access controls are rarely put in place for medical devices. Currently, there is no clear, orchestrated multi-disciplinary approach to securely managing medical devices on a network, let alone on multiple networks under various owners.

1.4. DEVICE VULNERABILITIES

Wearable wireless mHealth device shipments are forecast to reach 52 million worldwide by 2021

ABI Research calculates that there will be a total of 14.8 million wearable wireless mHealth devices shipped by 2016. This includes home monitoring, remote patient management, and professional on-site healthcare devices. The figure is set to more than triple, reaching 52 million globally by 2021. With low cybersecurity implementation, it is highly likely that the vast majority will include at least one, if not more, vulnerabilities. The incorporation of these devices into hospital networks means that they can, and will open up vulnerable access points to the entire infrastructure. With the proliferation of the medical IoT, it is only a matter of time before such devices are successfully exploited.

Currently, medical devices suffer from numerous vulnerabilities, and many devices do in fact compound several critical vulnerabilities, from within the application and software to the configuration and implementation mechanisms. Table 2 below lists various vulnerabilities that are commonly found in medical devices.

Table 2: Medical Device Vulnerabilities 2016

(Source: ABI Research & Mayo Clinic)

Operational	Application	Configuration	Software	Encryption
Limited customer support	Generally fragile applications	Unneeded ports and services enabled	Code errors in software/firmware	PHI & PII stored unencrypted
Poor internal technical documentation	No or easy passwords	Unneeded files and applications left on systems	Running an older OS with no upgrade paths	Communication is unencrypted
Limited publicly available information	Required to run with elevated privileges	Default users and passwords not removed or changed	Unpatched middleware with published exploits (JBoss, WebSphere)	Weak wireless encryption
Devices publicly available for purchase	Use hardcoded passwords	Disabled Windows firewall	Unpatched commercial applications with published exploits (Adobe)	Lack of authentication mechanisms
Customer service engineering	Incompatible with AC	Default settings on software and hardware	No or resource intensive process for updates and patching	Poor implementation (especially key management)
	Weak or non-existent input validation	Old communication and transfer protocols		
	Vulnerable to large number of known exploits (XSS, buffer overflows)			

Attackers can potentially use a variety of methods to gain access to medical devices. Often, they will use the simplest methods, and with security levels on average pretty low in the industry, it requires only relatively low hacking skills. Many legacy devices will also run obsolete systems (*e.g.*, Windows XP, which Microsoft stopped supporting as of 2014). This means that there will be no official patching support for new vulnerabilities, making it even easier for a potential attacker.

Where patches do exist, vulnerabilities remain. For example, the MS08-067 remote code execution exploit is often found in medical devices, despite a patch being out since 2008. Finally, there is a culture of "quiet patching." OEMs are reticent to publicly announce a security issue, even if they have pushed out an updated patch. As a result, those healthcare providers are often unaware of the importance of making the update, leaving a vulnerability open that could otherwise be easily remedied.

Vulnerabilities are often due to a lack of password protection or strength, which becomes critical when it concerns patient safety

While there are no known instances of a patient's medical device being compromised maliciously, the medical devices with the highest recorded number of vulnerabilities include infusion pumps, implantable cardiovascular defibrillators (ICDs), and CT scans. Often, the vulnerabilities are due to web administration interfaces that are not password protected or have weak passwords that are easy to crack. Unfortunately, this state of affairs is a recurring issue in many industries, and can become critical when patient safety is on the line.

Despite what appear to be glaring vulnerabilities, it is unrealistic to expect healthcare providers and device manufacturers to be able to mitigate all vulnerabilities of the devices under their purview (especially for larger providers who may have hundreds, or even thousands, of connected devices). While it may seem the security onus should weigh more heavily on manufacturers, many OEMs are small (80% of OEMs have fewer than 50 employees) and will not have the necessary knowledge or know-how in terms of cybersecurity to factor that into product development and testing. There is a definite lack of awareness among device manufacturers, as well as healthcare providers, about the need to identify and mitigate cybersecurity vulnerabilities in medical devices.

1.5. THREAT CONTEXT

The healthcare industry is at an all-time high for being a target of cyberattacks and monitoring equipment is at risk

Threat actors have been highly proficient at penetrating the healthcare infrastructure. Breaches in the industry are at an all-time high and healthcare is one of the top targets for cyberattackers. In 2015 alone, over 100 million health records were compromised globally. Three of the largest data breaches ever recorded in the sector occurred that year, with 79 million records breached at Anthem, and at least 10 million records each at Premera Blue Cross and Excellus Health Plan.

There are various motivations for attacks (financial, political), but for healthcare, the vast wealth of personally identifiable information makes it attractive for black market resale. More recently, ransomware has proven an extremely popular blackmail mechanism. Threatening to degrade medical devices or force them offline in a hospital setting is a highly lucrative course of action for a threat actor. In fact, healthcare providers have already been targeted by such attacks, although not many choose to make them public. However, there have been some publicized cases. Earlier this year, the Hollywood Presbyterian Medical Center in the United States paid a US$17,000 ransom in Bitcoin to an attacker who seized control of the hospital's computer systems and blocked access to patient records. Others have been similarly affected, including the Los Angeles County Department of Health, Chino Valley Medical Center, Desert Valley Medical Center, Methodist Hospital in Kentucky, and MedStar. While the attacks focused on the healthcare IT infrastructure, it will not be long before such attacks target healthcare monitoring equipment directly.

Undeniably, networked medical devices are vulnerable to attacks that can potentially lead to the failure to deliver appropriate care, or allow an attacker to maliciously alter device functionality. Healthcare providers have to understand that there is a new hostile environment that will emerge around networked medical devices and that threat actors have multiple levels of skills and diverging motivations. The average time from infiltration to discovery is 6 months for IT systems, and this is an informed threat landscape. For those players unaware of the risks, the window will be significantly longer, especially for devices that are still low on the radar for cybersecurity.

Currently, most efforts at exploiting and hacking medical devices are limited to proof of concepts by security researchers. As mentioned previously, there are no publicly known instances of malicious attackers successfully degrading medical devices in a care setting. This absence does not negate the existence of risk or the probability of such an event occurring in the future. The advantage of proof of concepts is that it can help qualify those risks; this is crucial for raising awareness and information about the reality and seriousness of insecure medical devices.

Table 3 below lists various publicized demonstrations of attacks on connected medical devices that have surfaced in the last few years.

Table 3: Notable Medical Device Hacks
Proof of Concepts and Research
(Source: ABI Research)

Researcher	Device	Method/Vulnerabilities	Year
Kevin Fu	Implantable Cardiac Defibrillator	Vulnerable *via* hard-coded passwords & RF replay attacks	2008
Jerome Radcliffe	Continuous Glucose Monitor, Insulin Pump	Interception of the unsecured wireless communication; protocol analysis & reversing required to understand security posture	2011
Barnaby Jack	Insulin Pumps	Ease of impersonation attacks	2012
Terry McCorkle, Billy Rios	X-ray Machines	Rudimentary fuzzer gave them privileged user status	2013
Billy Rios	Drug Infusion Pump	Forge drug library updates, unauthenticated telnet shell to root to the communications module, identical hardcoded credentials, identical private keys, identical encryption certificates	2014
Scott Erven, Mark Collao	Misc. & Honey Pots	Discovered 68,000 medical systems from a large unnamed U.S. health group on Shodan; Created honeypots impersonating MRI and defibrillator (acted as honeypots with attracted thousands of hackers, with 299 attempts to install malware)	2015
Sergey Lozhkin	MRI Device	Gained access to the device through the clinic's critical infrastructure using Wi-Fi network	2016
Billy Rios, Mike Ahmadi	CareFusion's Pyxis Supply Station	1,400 vulnerabilities discovered in the firmware (DHS ICS-CERT issued subsequent advisory)	2016

While hacking is a serious threat, it is not the only one. More worrisome is the problem of malware. Medical devices host numerous bugs and vulnerabilities, so any malware that may be present on a healthcare provider's network could easily infect such devices, regardless of whether they were the original target. Ransomware or a targeted DoS attack could effectively be leveraged against such devices. There have been previous cases of closed circuit televisions (CCTVs) being used in a DoS attack, and connected home goods (such as smart refrigerators) sending out spam. The possibility of medical devices being used for such purposes cannot be discounted.

In fact, cybersecurity firm TrapX published a report in 2015, *Anatomy of an Attack: Medical Device Hijack (MEDJACK)*, in which it revealed that a blood gas analyzer, a picture archive and communications system (PACS), and an X-ray system analyzed in three different hospitals showed malware infection, most disturbingly from complex and highly dangerous strains (including ransomware, Zeus, Citadel, and Conficker).

While there is a wealth of threat intelligence in the security market on vulnerabilities, malware, threat groups, and motivations, the problem is how to make sense of that information for the healthcare industry. In particular, how can stakeholders extract actionable intelligence specifically for medical devices? Having information on risk is important, but it needs to be followed up by information on how to mitigate it. The context around a vulnerability and the impact on clinical care will help define the risk to the patient and the operating environment. Following on from that must be information on mitigating controls, such as what can be reasonably done by a healthcare provider and/or a manufacturer to minimize risk.

1.6. PUBLIC HEALTH ISSUE

The healthcare industry needs to appreciate a number of key issues if they want to adequately address cybersecurity for medical devices. The first issue is the expansion of the medical IoT and the challenges resulting from diversity and connectivity. The second issue is the need to understand the evolving threat landscape and the risks to the device, to the infrastructure, to the patient, and to the provider. The final issue is determining risk acceptance and what can be done in terms of mitigation. It could be patching a device, unplugging it from the network, or simply leaving it as such.

The broader argument is that medical device cybersecurity should be recognized as a public health issue and one of growing critical importance. Cybersecurity involves numerous agents, many of which will not necessarily be versed in the field. Stakeholders include medical professionals, healthcare providers, device manufacturers, biomedical engineers, application/software developers, systems analysts, IT healthcare infrastructure staff, quality and risk officers, service providers, insurance providers, pharmaceutical companies, government organizations, and security companies.

The industry is already experienced in dealing with complex policy issues and regulatory compliance; therefore, tackling cybersecurity should not be an impossible task. The methods for dealing with forthcoming cybersecurity issues can find footing in traditional public health practice. But it requires the participation of all healthcare stakeholders.

Cybersecurity should be included as an integral part of the medical IoT, along with managing quality, usability, and lifecycle

Unfortunately, security and risk are not the only issues for providers dealing with the medical IoT. The current focus is on managing quality, usability, and lifecycle. These often take precedence over cybersecurity considerations. Research, development and testing looks first to assuring patient care, and while cybersecurity is part of that discussion, it is not the principle concern. Making cybersecurity a public health issue would drive increased awareness and action in the space.

The following section looks at initial efforts, both public and private, in cybersecurity for medical devices, as well as market trends in terms of spending and service revenue.

2. IMPLEMENTING MEDICAL SECURITY AND SAFETY

Healthcare delivery organizations are tasked with delivering safe and effective healthcare. This becomes increasingly difficult as networked medical devices proliferate. Despite introducing improvements in healthcare delivery, they also introduce risks that can affect patient safety, as described in the previous section.

Protecting devices requires addressing technical issues, healthcare delivery, and business challenges, and this collaboration across the various stakeholder silos is necessary. The industry, however, is at the beginning stages of the discussion. Globally, the efforts are poor, and the United States is the only country currently putting significant energies into the matter. This is not surprising as almost half of medical device manufacturers are based in the United States. This is not to say that the healthcare industry is not incorporating cybersecurity as a whole. On the contrary, both in Europe and in North America, there a raft of data protection and regulatory compliance mechanisms are in place for the sector, which has driven increased spending in the space.

2.1. HEALTHCARE CYBERSECURITY SPENDING

Global expenditure in cybersecurity for the healthcare sector as a whole is estimated to reach US$5.5 billion by the end of 2016. This amount will double by 2021, with US$11.6 billion spent globally by healthcare providers, emergency medical services, pharmaceuticals, OEMs, government agencies, and other stakeholders (health plans, clearing houses, business associates, and insurers).

Only 8% of global spending on cybersecurity is attributed to the healthcare industry in 2016

However, this represents only a fraction of the trillion-dollar spending on healthcare generally as estimated by the World Bank and the OECD (as mentioned earlier in this report). Even in comparison to total spending on cybersecurity for protecting the critical infrastructure, healthcare represents only 8% of the global total, which is estimated at US$65 billion in 2016. It sits alongside the energy industry and the water and waste management sector in terms of the least amount of spending on cybersecurity.

Table 4 below illustrates spending on healthcare cybersecurity as a whole. See ABI Research's report on *Critical Infrastructure Security: Healthcare* and the *Critical Infrastructure Security* market data for more information.

Table 4: Healthcare Critical Infrastructure Cybersecurity Spending
World Markets, Forecast: 2016 to 2021 *(Source: ABI Research)*

Segment	Revenue	2016	2017	2018	2019	2020	2021	CAGR 16-21
Healthcare	(US$ Billions)	5.50	6.15	7.54	8.84	10.37	11.68	16.3%

The main reason for the massive lag in spending, despite obvious regulatory drivers, is that the healthcare industry has focused almost exclusively on data protection, to the detriment of protecting networks and systems. And there is even less in the way of actually protecting medical devices. Despite this, the CAGR for the 2016 to 2021 period is forecast at 16.3%, higher than most other critical infrastructures, including finance, defense, ICT, and energy.

This dynamism is due in part to the growing awareness of the severe gap in security technologies as the healthcare industry tries to counter ever frequent data breaches. It is also due to the growing conversion of health records to digital formats, and in the United States notably, the number of insured people, driving the need for increased spending, even if the industry as a whole does not reach the security level found in other sectors.

2.2. PUBLIC EFFORTS: THE UNITED STATES SHINES

The public sector in the United States is playing the biggest role globally in advancing cybersecurity for medical devices, increasingly supported by private sector players. Many of the initiatives started with regulation specific to healthcare, notably the Health Insurance Portability and Accountability Act (HIPAA) for the security and privacy of health data; the HITECH Act, which extends the scope of protections for HIPAA; and the Federal Trade Commission (FTC) "Red Flags Identity Theft Prevention Rules." These form the most important pieces of legislation regarding the protection of medical records in the United States.

In the European Union (EU), there are directives that drive compliance: the Medical Devices Directive 93/42/EEC; the Data Protection Directive 95/46/EC (which is currently being revised); the Privacy and Electronic Communications Directive 2002/58/EC; and the Cross-border Healthcare Directive 2011/24/EU; all of which confer a number of articles on data protection and security. However, there has been limited movement in terms of medical device cybersecurity. Both the EU and the United States have harmonized internally the international standard IEC 62304 on medical device software (lifecycle processes) and there is discussion around updating it in terms of security.

U.S. directives have been designed to mobilize both the public and private sectors to strengthen cybersecurity infrastructure

The real drive, however, is taking place in the United States as a result of the White House Executive Order 13636 on "Improving Critical Infrastructure Cybersecurity" and the Presidential Policy Directive 21 on "Critical Infrastructure Security and Resilience," both issued in 2013. The idea was to mobilize both the public and private sectors to collectively strengthen critical cybersecurity infrastructure.

2.2.1. THE FDA

The Food and Drug Administration (FDA) has acted accordingly, with a number of recommendations and guidance papers, including: "Cybersecurity for Medical Devices and Hospital Networks" (2013); the "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (2014); and "Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software."

The goal of the recommendations are generally for code verification for software and firmware updates, encrypting data transmission, developing and implementing processes for detecting, communication, and responding to events. As of yet, the FDA has not drafted any regulation in the space, and the industry does not expect any to be forthcoming. There is a general consensus in the United States that regulation could stifle innovation.

Going forward, however, the FDA continues to provide recommendations in the space. Most recently, in January 2016, the FDA released draft guidance on "Postmarket Management of Cybersecurity in Medical Devices," which was open to comments for 90 days and will see a final publication in the near term. Table 5 below provides an overview of the main points for the FDA's pre- and post-market guidance.

Table 5: FDA Review of Pre- and Post-market Guidance for Cybersecurity in Medical Devices 2014 and 2016 *(Source: ABI Research)*

Content of Pre-market Submissions for Management of Cybersecurity in Medical Devices, 2014	**Post-market Management of Cybersecurity in Medical Devices, 2016**
Consider cybersecurity risks when designing and developing medical devices	Implement a structured and systematic comprehensive cybersecurity risk management program and respond in a timely fashion to identified vulnerabilities
Provide the following information: hazard analysis, mitigation and design considerations, traceability matrix, plan for validating software updates, summary of controls in place, device instructions for use and product specifications	Applying the 2014 NIST Voluntary Framework for Improving Critical Infrastructure Cybersecurity, which includes the core principles of identify, protect, detect, respond, and recover
Identification of assets, threats, and vulnerabilities	Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk
Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients	Understanding, assessing, and detecting presence and impact of a vulnerability
Assessment of the likelihood of a threat and of a vulnerability being exploited	Establishing and communicating processes for vulnerability intake and handling
Determination of risk levels and suitable mitigation strategies	Clearly defining essential clinical performance to develop mitigations that protect, respond, and recover from the cybersecurity risk
Assessment of residual risk and risk acceptance criteria	Adopting a coordinated vulnerability disclosure policy and practice
Consider the following cybersecurity framework core functions to guide their cybersecurity activities: identify, protect, detect, respond, and recover	Deploying mitigations that address cybersecurity risk early and prior to exploitation

The guidance also addresses the importance of information sharing *via* participation in an Information Sharing Analysis Organization (ISAO), a collaborative group in which public and private-sector members share cybersecurity information. Further, the FDA does not intend to enforce urgent reporting of the vulnerability to the agency if certain conditions are met. One of these conditions is the participation in an ISAO and subsequent reporting of the vulnerability to the group.

In an effort to drive collaboration, the FDA entered into a memorandum of understanding (MoU) in 2014 with the National Health Information Sharing and Analysis Center (NH-ISAC), a nonprofit health sector-led organization that provides member organizations with actionable information on cybersecurity and coordinates cybersecurity incidence response. And most recently, in June 2014, the NH-ISAC entered into a partnership with the Medical Device Innovation, Safety and Security Consortium (MDISS) to meet the goals of the MoU in terms of fostering stakeholder collaboration.

Together, the two nonprofits launched the Medical Device Information Sharing and Analysis Initiative as an extension of the Device Information Sharing Council that they co-chair under the umbrella of NH-ISAC. The initiative will provide coordinated information and analysis to support timely response activities by stakeholders (including healthcare providers and OEMs). Information sharing will include medical device risk assessments, host vulnerabilities, and threat intelligence.

A number of companies have already committed to membership, including Abbott, AdvaMed, Baxter, Boston Scientific Corporation, GE Healthcare, Intuitive Surgical, Johnson & Johnson, Royal Philips, and St. Jude Medical.

Alongside the various issued reports, the FDA has also organized a series of workshops over the years, the latest being held in January 2016 on medical device and healthcare cybersecurity to discuss the various FDA guidance tools. The MITRE Corporation (MITRE) has since set up a website group on “Collaborative Approaches to Medical Device and Healthcare Cybersecurity.” It is essentially a virtual collaboration space for interested stakeholders to continue the dialog.

2.2.2. THE DHS

Aside from the FDA and its numerous efforts, other agencies are also issuing alerts on the security of medical devices in the United States, including by the Department of Homeland Security (DHS) (Medical Devices Hard-Coded Passwords in 2013) and the FBI (Private Industry Notification: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain in 2014).

The DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) also revealed in 2014 that it investigated about 24 cases of cybersecurity vulnerabilities in a wide range of medical equipment, from medical imaging devices to hospital networking systems, including Hospira Symbiq infusion pumps and Medtronic’s implantable heart devices. ICS-CERT is working with OEMs to help them identify and repair the vulnerabilities. In fact, the team has been coordinating with the FDA since 2013 across all the stakeholders within the medical device ecosystem.

2.2.3. OTHER ORGANIZATIONS

The United States is seeing cybersecurity initiatives by federal organizations, private companies, and industry alliances and associations

The level of awareness in the United States is higher than in any other country currently, with such efforts being accompanied by industry alliances and associations, such as the Health Information Trust Alliance (HITRUST) and the American Hospital Association (AHA). Two other organizations of notably interest have also emerged in the space: I Am The Cavalry and the Medical Device Cybersecurity Taskforce.

I Am The Cavalry is a grassroots organization focusing on the impact of cybersecurity, public safety, and human life. The group focuses on various sectors, including home, public infrastructure, automotive, and medical, and has numerous members and partners among the technology industry and government agencies. Specifically in the medical space, I AM The Cavalry focuses on topics such as implantables, telemetry, imaging, diagnostic, radiology, nuclear medicine, and home healthcare. The association published an open letter in January 2016 to the healthcare stakeholder communities urging them to:

- Acknowledge that patient safety issues can be caused by cybersecurity issues
- Embrace security researchers as willing allies to preserve safety and trust
- Attest to these five foundational capabilities to improve visibility of their Cyber Safety programs
- Collaborate now to avert negative consequences in the future

I Am The Cavalry has also drafted a Hippocratic Oath in 2016 for connected medical devices to help develop key areas of controls and capabilities and lay the groundwork for improving medical device cyber safety. The Oath contains five key principles: cyber safety by design, third-party collaboration, evidence capture, resilience and containment, and cyber safety updates. The group has done much to raise awareness of the functional safety and cybersecurity concerns of the new threat vectors in both automotive and medical, and is illustrative of the importance of grassroots movements in a sector that can easily be polarized by unilateral private *versus* public sector efforts.

The Medical Device Cybersecurity Task Force (MDCTF) was set up at the end of 2015 and is a voluntary organization that consists of healthcare organizations and security firms. Founding members are Sensato and Divurgent, with membership now including 63 different organizations. The task force focuses on developing and sharing:

- Best practices related to securing medical devices from cyberattackers
- Threat intelligence related to medical device cybersecurity attacks
- Collaborative and trusted channels for communication related to medical device cybersecurity

While driven by economic interests, collaboration among vendors and healthcare providers is necessary

The goal is to provide short-term practical improvements as they relate to computers, network security, and medical devices. This can be done by applying existing standards and best practices, such as those developed by NIST, the FDA, or ISC2 to medical security. The issue is essentially an economic one, notably due to devices numbering in the thousands, their long lifespans, and the potential liability of both OEMs and healthcare providers. Membership is open to all vendors and healthcare providers that are interested, and the task force organizes four meetings a year to strengthen collaboration and information exchange. The creation of the task force is an important development in terms of private sector engagement in the field and shows willingness to cooperate, despite intense competition in the market, on a critical area of research.

2.3. DEVELOPMENT CONSIDERATIONS

The results of these various discussions, initiatives, and best practices have started to shape a picture of how medical devices can be better secured against cyberthreats. In theory, much of it can, and has been, mirrored on existing security development lifecycle processes, such as those developed by the U.S. NIST (Special Publication 800-64 Revision 2) or Microsoft (Security Development Lifecycle). There are several stages at which security needs to be considered, and while they may vary according to the different practices, they can be more or less split into two broad groups: pre- and post-market.

In pre-market considerations, a manufacturer or developer should ideally go through three stages: designing security, incorporating security, and testing security. These phases should be accompanied by various risk management exercises in order to fine-tune cybersecurity requirements. Specifically within medical devices, both hardware and software considerations are numerous. In hardware, a greater variety of highly diverse products are available: from small sensors and embedded systems with little or no firmware, to large complex machines running Linux or Windows operating systems.

For post-market considerations, the main goal is to maintain security throughout the product's lifecycle. This means monitoring the state of security, making appropriate modifications and enhancements, putting in place an incident response plan, and continually auditing and reviewing the product. In this scenario, manufacturers have to develop methods to provide secure updates, to patch vulnerabilities efficiently and quickly, and perhaps even to put into place vulnerability disclosure or other bug bounty programs. Information sharing with security researchers, CERTs, law enforcement, and other OEMs can play a crucial role in maintaining cybersecurity over the course of the device's life.

Overall, medical device manufacturers are forecast to spend US$390 million globally on pre- and post-market cybersecurity implementation, reaching US$1.19 billion by 2021. This includes everything from embedding security in the hardware, review, analysis, pen testing, patch development, and OTA updates, among other functions, which will be done sometimes internally, but primarily through third-party services. Table 6 below illustrates global spending over the forecast period.

Table 6: Medical Device Security Spending
World Markets, Forecast: 2016 to 2021 *(Source: ABI Research)*

Segment	Spending	2016	2017	2018	2019	2020	2021	CAGR 16-21
Medical Device Security	(US$ Billions)	0.39	0.49	0.64	0.80	1.01	1.19	25.4%

2.4. SECURITY MAINTENANCE

Healthcare providers need to be aware of how to take advantage of a device's security features

Having a secure medical device does not guarantee security. Once a healthcare provider has the device in hand, it needs to be able to take advantage of the security features and to implement additional security mechanisms and management functions, including: device control, system protection, application security, transmission and communication security, device identity, authentication and access control policies, provisioning and managing encryption keys, detecting and acting on intrusions or adverse events, managing trust, protecting data, conducting risk assessments, creating an incident response plan, educating medical professionals on proper usage, obtaining and sharing information on threats and vulnerabilities, *etc*.

The list is long and certainly non-exhaustive, requiring investment and resources. The devices are so diverse, so not all security considerations are applicable, but healthcare providers need to come to terms with this complexity. Further, they need to ensure integration of these security functionalities with their own value chain, including contractors, third parties, and other service providers.

ABI Research estimates that healthcare providers and other caregivers will spend US$3.19 billion on IT networks, systems, and data security, and just over half that (US$1.93 billion) on implementing security processes, as well as educating and training healthcare professionals in 2016. By 2021, spending is forecast to reach US$6.32 billion and US$4.71 billion, respectively. Table 7 illustrates spending in these segments.

Table 7: Healthcare IT Security Spending
World Markets, Forecast: 2016 to 2021 *(Source: ABI Research)*

Segment	Spending	2016	2017	2018	2019	2020	2021	CAGR 16-21
IT Network, Systems, & Data Security	(US$ Billions)	3.19	3.51	4.26	4.95	5.76	6.32	14.7%
Process & Personnel	(US$ Billions)	1.93	2.15	2.64	3.09	3.61	4.17	16.7%

The primary focus for IT systems will remain the protection of data, although increasingly over the forecast period, network-level security aimed at managing medical devices will be covered. Currently, however, the percentage allocated to medical devices is low and will remain so over the entire forecast period. Healthcare providers will rely on OEMs to integrate cybersecurity within medical devices and will not expend significant resources on security management in the short term. Most providers are still very much concerned with protecting data and implementing the requirements, at least in the United States with HIPAA and HITECH. This means financial resources will not be diverted to the security maintenance of medical devices in the foreseeable future.

The initial focus is on complying with data protection legislation, with security management and maintenance following eventually

Similarly, spending on processes and personnel will not immediately involve training in securing medical devices on premise. Currently, the focus is on complying with data protection legislation, and therefore, training medical professionals in this area first. In the longer term, as collaboration between various stakeholders' increases, notably between security professionals, biomedical engineers, healthcare CIOs and CSOs, system administrators, and medical professionals, more comprehensive training will eventually encompass the security management and maintenance of connected medical devices.

2.5. HEALTH MONITORING SECURITY SERVICES

The increased connectivity of medical devices will force both healthcare providers and medical device manufacturers to focus on how best to secure devices remotely. Further, the eventual adoption of a secure development lifecycle will push for continuous monitoring and security maintenance. One of the more appealing options will be to outsource complex functions to service providers with expertise in cybersecurity.

Security services will initially be offered for home and patient monitoring scenarios

Security services as they relate to this sector will primarily emerge around home and patient monitoring, as these often represent complex management scenarios for healthcare providers: both incorporate concepts of remoteness and mobility, and will often fall outside of the control of the provider's network. This is where cybersecurity vendors, mobile network operators, OEMs, and emerging healthcare IT technology providers will step in to offer security services.

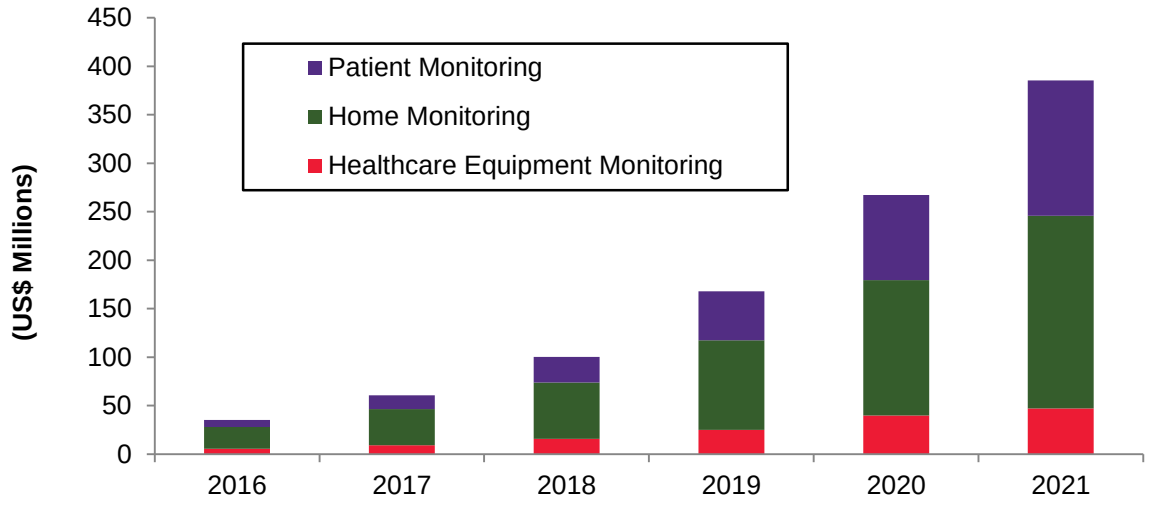
Healthcare equipment monitoring will be relatively less difficult to manage internally, and can be compared to mobile device management in theory. As seen in the enterprise space, service providers for medical device management will emerge to service this space.

Table 8 and Chart 2 below illustrate security services in the health monitoring space, which is forecast at US$35 million globally by the end of 2016, reaching US$385 million by 2021. All three segments will see significant CAGRs over the forecast period. Much of it is driven by the adoption of EHRs and the connection of medical devices with EHR databases for more streamlined care delivery.

Table 8: Health Monitoring Security Services Revenue
World Markets, Forecast: 2016 to 2021 *(Source: ABI Research)*

Segment	Revenue	2016	2017	2018	2019	2020	2021	CAGR 16-21
Healthcare Equipment Monitoring	(US$ Millions)	5.54	9.12	15.67	24.93	39.70	47.12	53.4%
Home Monitoring	(US$ Millions)	22.47	37.27	58.18	92.48	139.81	198.81	54.7%
Patient Monitoring	(US$ Millions)	7.35	14.20	26.33	50.53	87.85	139.30	80.1%
Total	(US$ Millions)	35.36	60.59	100.18	167.95	267.36	385.23	61.2%

Chart 2: Health Monitoring Security Services Revenue
World Markets, Forecast: 2016 to 2021 *(Source: ABI Research)*



These security monitoring services include revenue derived from security-related service-level agreements (SLAs). SLA offerings are dependent on the client and application, but generally include the integration of security management services into enterprise information services. This can include response virus/spam detection time to trouble calls, mean time between failures, average time to service help desk requests, contingency plans, backups (including archiving and restore), user training, and war games (such as penetration or social engineering), among others. However, such services are still relatively niche and are not used widely within healthcare.

Other services that can be offered include those for transport, where security is provided on three layers in the Open System Interconnection (OSI) model: data link, transport, and network levels. Transport security technologies offer authentication and encryption functionalities suitable for securing transmissions over different types of networks, from fixed to wireless, and through licenses purchased from certification authorities.

Finally, such services can also include physical security. This includes the protection of network components, medical devices, machines, and other sensors from physical threats, including theft, physical destruction, environmental conditions, and other adverse events. Security can also include enclosing the perimeter where the devices are located and installing surveillance mechanisms, such as CCTV.

2.6. A SLOWLY EMERGING PRIORITY

The U.S. healthcare industry's multi-stakeholder collaboration and research in tackling cybersecurity is admirable

Despite the obvious vulnerabilities of connected medical devices and the potential risk to patient safety, cybersecurity in this space is emerging at a slow pace. Most efforts, however small and recent, are U.S. based and stem either from security researchers or the U.S. government. There is little doubt that the U.S. government's drive in proactively tackling cybersecurity within critical infrastructures is a significant global driver in many industries, and the U.S. healthcare industry has pulled together admirably in terms of multi-stakeholder collaboration and research in this area. Other countries, notably in developed regions, would do well to follow the example and start tackling the issue before the medical IoT becomes entrenched and immutable. Investment in medical device cybersecurity now by OEMs and healthcare providers globally would enable them to form part of the ongoing discussion that will undoubtedly form the foundation of future cybersecurity practices in the sector.

3. CYBER READYING THE MEDICAL COMMUNITY

Despite policy and research advances, medical OEMs and healthcare providers are not yet implementing cybersecurity for medical devices in any coordinated or widespread manner. Various factors, as seen throughout this report, lend to this issue, including low levels of risk awareness, lack of knowledge and expertise, other compliance concerns, and cost and liability issues, among others. There are no standards or regulation in place to really drive the process forward.

However, in the last year or so, there have been some significant collaborative efforts to meet, discuss, and attempt to solve the issue. Various recommendations and best practices have been published, and not just by government and research and development (R&D) organizations. Medical OEMs and technology companies are leading in this space by example and a few of these are highlighted in this section: Battelle, Coalfire, Draeger, Extreme Networks, Sensato, Synopsys, UL, and WhiteScope. These are not the only players; others, not reviewed here, include Philips, Adventium Labs, and the MITRE Corporation.

3.1. BATTELLE

Battelle's DeviceSecure Services identifies vulnerabilities and works to resolve a wide range of cybersecurity issues

Battelle is a U.S. charitable trust focusing on R&D in national security, health and life sciences, and energy and environmental industries. The organization started orienting its research toward medical device security 5 years ago, and today offers a wide range of services, from testing to design. Its primary efforts in the space come under the Battelle DeviceSecure Services. These include secure design, vulnerability assessment, IP protection, anti-tampering, anti-counterfeiting, and integrated high-density embedded component assembly. Most importantly, Battelle looks at the software and hardware pieces in order to identity potential security vulnerabilities.

Battelle provides a comprehensive design process to increase the quality systems of medical device problems at the start. The organization leverages the NIST SP 800-53 standard to develop a security baseline for design and validation. For vulnerability assessment, Battelle provides risk management analysis of existing hardware and software vulnerabilities after the design phase.

The organization provides also auditing, architecture review, and testing for various phases, depending on feature sets and client requirements. Battelle seeks to refine its services by digesting best practices that are issued in the space, and applying lessons learned. Threat modeling for devices initially takes the same approach as for traditional IT devices. However, the focus will change depending on the type of threat, as the attack surface can differ vastly (large machine *versus* implantable device).

Battelle is working tightly with medical OEMs and is keen to push lifecycle management as well. Going forward, in addition to secure design and testing, it will look to tackle the issue of how to maintain security over the course of a device's life, focusing on implementing appropriate engineering and patching methods.

3.2. COALFIRE

Coalfire's cyber risk management and compliance services focus primarily on healthcare, payments, cloud, and technology

Coalfire is an independent risk advisory firm based in the United States. The firm provides cyber risk management and compliance services for various regulations and standards (PCI DSS QSA, ISO, HIPAA, FedRAMP, *etc*.). Coalfire focuses primarily on healthcare, payments, cloud, and technology. Services offered to the healthcare sector include application security services, DEA EPCS certification audit, HIPAA/HITECH assessment, HITRUST compliance services, cyber risk management, and penetration testing services.

Embedded medical technology is one of the areas covered by Coalfire; for example, within pacemakers and MRI scanners. Vulnerabilities within these areas are an ongoing issue, including concerns regarding liability. This is a relatively gray area for OEMs and healthcare providers, notably because existing regulation and compliance is around data and not devices. One of Coalfire's goals is to look at medical devices from a risk management perspective.

Coalfire works with a number of embedded technology vendors, taking an engineering approach and investigating very specific design considerations, such as power consumption, teardowns from a threat scenario perspective, fail-safe considerations, cloud management, monitoring, and clinical payloads, among others. The firm also looks at the issue of liability and how these various risks might hold up in court. Due to the relatively nascent market for such services, such considerations are determined on a case by case basis.

3.3. DRAEGER

Draeger is one of the most advanced medical OEMs in terms of implementing cybersecurity into medical devices. Cybersecurity is considered in every phase of the product lifecycle, from the idea to phase out. It starts with training of the participating roles (developers, architects, product managers, *etc*.). The firm does threat modeling, applies fuzz testing, static and dynamic code analysis, manual code reviews, and each product release usually goes through an external penetration test. After the product is in the field, the firm monitors various sources for cybersecurity vulnerabilities to make risk assessments, determining whether or not patching is necessary.

Draeger employs a number of teams to test cybersecurity, including teams that do security testing for the development teams, and development teams that do the security testing. In addition to these constant efforts, the firm does external pen tests with renowned cybersecurity professionals.

Draeger builds its product security strategy on OWASP's openSAMM and Microsoft's SDL framework. It also operates a coordinated vulnerability disclosure process according to ISO 30111 and ISO 29147. The firm is fully compliant with the FDA's pre-market guidance and almost fully compliant with the FDA's draft post-market guidance, even before it has been officially finalized. The firm also keeps a close watch on EU directives that are currently being discussed, but only very vague statements are mandatory for medical device manufacturers; ISO 62304 mandates, in section 5.2.2 in particular, a number of security requirements ("compromise of sensitive information, authentication, authorization, audit trail, and communication integrity").

Draeger supports healthcare organizations by providing documentation regarding the security of their products that they can integrate into their network infrastructures

Furthermore, the firm was actively involved in the writing of the technical report AAMI TIR57 (Risk Management) that bridges the gap from performing risk management only for patient safety-related cybersecurity issues to evaluating, information disclosure, and efficacy risks. Finally, Draeger also takes into consideration ISO 80001-1, a standard that applies to healthcare delivery organizations, in order to manage risks for IT networks containing medical devices. While the standard mainly does not apply to manufacturers, the firm does its best to support healthcare organizations by giving them sufficient documentation about the security of their products, so they can easily integrate them in their network infrastructures. Additionally, the Draeger Academy offers a workshop to train hospital IT staff to become certified risk managers for medical IT networks.

Draeger has put in place a guidance list (a sort of 10 commandments) for all products. Wherever possible, its products comply with the following list:

- Do not ship with (or rely on) discontinued, unsupported, or vulnerable components
- Run on the least possible privilege
- Ship in the securest state by default
- Do not ship with hard coded credentials
- Have security designed in from the beginning
- Are resilient against unexpected inputs on any of their interfaces
- Are designed to protect all data, at rest and in transit
- Have no hidden backdoors, debug ports, or unnecessary software running
- Are designed to receive security patches
- Protect critical functions from unauthorized access

Draeger also has a list of concrete global security requirements, binding for all products being developed. In addition, it constantly trains its development team and field staff in security. Its current challenges are to speed up security patch development and patch rollout for already deployed products and to even further improve the security of legacy products.

3.4. EXTREME NETWORKS

Extreme Networks is a manufacturer of network infrastructure. While the traditional focus has been on hardware, the firm has expanded considerably into the software and cloud business to control and automate infrastructure. Extreme Networks offers a range of solutions for healthcare, including application and intelligence control, clinical grade BYOD, and IoT and medical device safety.

Extreme Networks provides its already existing solutions that are tailored to and simplified for its healthcare provider clients

The firm essentially deploys its existing solutions and tailors them to a healthcare setting. These include: ExtremeSwitching, Extreme Management Center, ExtremeWireless, Extreme Access Control, and Extreme Analytics. The goal is to enable healthcare providers to have centralized visibility and end-to-end control of the unified network, hybrid deployment architecture, SSO, policy controls, embedded flow-based ASIC flow sensor technology per port, 3M flows/sec collection capability, automated and secure provisioning and control of medical devices on the wired/wireless network, and agentless performance and security monitoring of medical device communications, among other features. The firm also offers professional services, maintenance, and customer training, as well as a 24/7 Global Technical Access Center.

Extreme Networks has built into its existing solution the ability to discover new devices and end systems, build a profile around then, determine risk, and apply authentication mechanisms. Its solutions can make use of various policies to isolate devices before defining access policies. The software intelligence element of the solutions provides the automation. For Extreme Networks, the goal is to abstract away complexity and to provide simplified and intuitive tools for healthcare providers.

3.5. SENSATO

Sensato is a cybersecurity company focused on providing solutions for the healthcare industry. The firm offers a range of services that cover compliance and strategy, education and simulation, testing and validation, emergency response, and managed services. The firm is behind one of the first healthcare industry conferences on cybersecurity (Hacking Healthcare) and is one of the founding members of the Medical Device Cybersecurity Task Force.

Sensato launched its CTOC for healthcare in 2016 to provide industry-specific security operations and research

Most recently, in 2016, the firm launched an industry-specific security operations and research center called the Sensato Cybersecurity Tactical Operations Center (CTOC) for healthcare. The CTOC will offer services covering intelligent SIEM, behavioral monitoring, threat detection, asset discovery, vulnerability assessment, collaboration, advanced intelligence, and emergency response.

3.6. SYNOPSYS

U.S. firm Synopsys focuses on electronic design automation, semiconductor IP, software quality, and security services. The Software Integrity Platform offers various application security solutions, including software composition analysis (Protecode), static code analysis (Coverity), intelligent fuzz testing (Defensics), runtime security analysis (Seeker), automated test optimization (Test Advisor), and actionable threat intelligence (AbuseSA). The acquisition of Codenomicon in 2015 enabled Synopsys to reach this breadth of security offerings and provide more comprehensive tools for cyber supply chain management.

Synopsys researches discovered 1,400 vulnerabilities in the medical supply station, forming the basis for the ICS-CERT advisory this year

Synopsys's platform is being used to test medical devices. In fact, researchers at the firm are behind the recent discovery of the 1,400 vulnerabilities in the medical supply station, which formed the basis of the ICS-CERT advisory earlier this year. The tools can be effectively used to test code for quality and for security issues within medical devices. The firm works very closely with the FDA and the ICS-CERT, sending found vulnerabilities to those organizations on a regular basis, as well as with progressive medical OEMs, such as Philips and the Mayo Clinic.

Synopsys has further drafted a Procurement Language for Supply Chain Cyber Assurance document that is available freely. It is currently being evaluated and deployed by multiple organizations and describes the methods for the evaluation of network-connectable devices and the testing for known vulnerabilities and software security weaknesses. The goal of the document is to establish a minimum set of verification activities for the various software types in order to reduce the likelihood of exploitable weaknesses. Synopsys bases the requirements on various industry standards and guidelines, including those from the IEC, ISO, NIST, DHS, ISA, FIPS, CC, Mayo Clinic, and UL.

3.7. UL

UL is a U.S.-based company offering science expertise in numerous areas, including analytical chemistry, biomedical engineering, clinical science, compliance engineering, electrical engineering, EMC & wireless, global regulatory, readiness & remediation, human factors engineering, quality, regulatory research, risk management, software, cybersecurity, interoperability, supply chain audit, inspections, toxicology, and user experience.

The firm has a long history in working with embedded software, microcontrollers, and software in the safety space. Already in 2008 to 2009, UL started investigating the technology-specific risks as they related to functional safety. In 2015, U.S. government agencies initiated the discussion around a program suggestion, and the development of general requirements and specifications in the ICS and healthcare sector. The idea was to align such efforts with existing standards and practices, notably risk management, and at the network and system level.

UL's CAP launched in March of 2016 in conjunction with academia and industry consortiums and is the first of its type focused on healthcare

As a result of these discussions, the UL Health Science Solutions for Software, which focuses on interoperability, quality, and security, started work on the UL Cybersecurity Assurance Program (CAP), and specifically CAP for Healthcare Products (UL 2900-2-1). The CAP was officially launched at the end of March 2016, and was developed in conjunction with academia and industry consortiums. It is the first program of its type focused on healthcare.

The CAP is aimed for use in hospital procurement processes to reduce vulnerabilities and malware, and to increase security awareness. The program includes a number of tools to help establish a bill of materials showing software components. It makes use of existing processes for risk management, QMS, and SDLC (notably from the ISO and IEC), and is aligned with regulatory processes (FDA and ISO). UL engages in the disclosure of CAP results in order to support the supply chain. This can be done publicly *via* the web, or privately *via* a NDA. Going forward, UL is preparing to launch a stakeholder group under the program.

3.8. WHITESCOPE

WhiteScope is a pioneer in providing training and security services, offering healthcare, 510(k), and medical device assessment

WhiteScope specializes in expert training and professional security services for various sectors. In particular, the firm offers healthcare, 510(k), and medical device assessment. The firm is a pioneer in the space. WhiteScope researchers were the involved in first FDA cyber security advisory and one of the first FDA 510(k) cybersecurity submissions.

Some of the tools created by WhiteScope include last-mile supply chain validation and GroundTruth Hunter Tools (for proactive hunting operations for unauthorized entities). It is currently working on an embedded device identity tool, which is coming soon.

The firm has been at the forefront of IoT security research, and earlier in 2016, it won a nearly quarter-million-dollar DHS award Under the Silicon Valley Innovation Program (SVIP) Other Transaction Solicitation (OTS) to create a wireless communications gateway aimed at protecting the IoT. WhiteScope's GatewayX will create an IoT communications portal specific to connected devices, sensors, and networks and will meet IEEE 802.11 standards.

4. RELATED RESEARCH

MD-IOTMWW-102	IoT Market Tracker - Worldwide
MD-CIS-159	Critical Infrastructure Security
MD-WHEA-111	Wireless Healthcare and Fitness
AN-1411	Critical Infrastructure Security: Healthcare
AN-1946	IoT Services for Medical Imaging Equipment Market: MRI, X-ray, CT Scanners, and Tomography

Published October 11, 2016

South Street
Oyster Bay, NY 11771 USA
Tel: +1 516-624-2500
www.abiresearch.com