The Medical Device Paradox

Hospital Systems and Device OEMs Race Against Time to Close the Patient Safety Cyber Gap

CYLANCE™

Introduction

Trust. It is what makes the world go round. As the Internet of Things (IoT) continues to grow exponentially, there remains an underlying need to trust the security of services, technologies, and relationships that — in a perfect world — ensure the continuity of everyday living.

In a November 2015 report by Gartner, Inc., researchers forecasted that 6.4 billion connected 'things' will be placed in everyday use by the end of 2016. That number is projected to grow to 20.8 billion by the year 2020. According to the Information Systems Audit and Control Association (ISACA), the medical devices industry is one of the top IoT markets to be hit by cyberextortionists in 2016. Security breaches make headlines daily; however, advanced persistent threats within the healthcare and medical device markets represent more than the exploitation of protected health information (PHI).

A May 2015 study on privacy and security of healthcare data conducted by the Ponemon Institute revealed that criminal motivations are the leading drivers behind healthcare data breaches. Cybercriminals include those seeking financial profit as well as Snowden-like hacktivists and nation states who leak private information or threaten data integrity as leverage for geopolitical or economic gain.

Healthcare records garner higher value on the black market versus financial account records. Reuters reported in 2014 that medical information was worth 10 times more than credit card information on the dark web. Cybercriminals have become the catalysts for high-value fraudulent transactions, including controlled pharmaceuticals. Unlike the financial services industry, healthcare providers often lack mature fraud-monitoring capabilities, and therefore, healthcare breaches result in a greater yield for cybercriminals.

In the absence of proven endpoint protection, medical device vulnerabilities can represent a threat greater than just financial loss in the potential for loss of life.

On May 19, 2010, the assistant secretary of information and technology for the U.S. Department of Veterans Affairs made this statement before Congress following his postmortem of threats to the VA's medical devices: "Over 122 medical devices have been compromised by malware over the last 14 months. These infections have the potential to greatly affect the world-class patient care that is expected by our customers. … These incidents are also extremely costly to the VA in terms of time and money spent cleansing infected medical devices."

Four years later, an exposé in the technology magazine, Wired, revealed the results of a two-year study by Essential Health. During this study, significant security vulnerabilities were documented within a large range of medical devices including drug infusion pumps and defibrillators as well as X-ray and digital medical record systems.

The number of malware samples discovered each year continues to reach record numbers with the latest estimates hovering around 300 million new strains detected in 2015.

The Growing Paradox of Medical Device EFFICACY

Network Configuration & Software Design Flaws

In an attempt to move quickly in an aggressively growing market, medical device manufacturers may compromise on risk management practices. This problem can be complicated by the reliance on a complex global supply chain and vendor network to ensure that the proper authentication, authorization, and data integrity requirements are satisfied. Cybercriminals are able to utilize malware to exploit vulnerabilities and attack with the intent of acquiring PHI, directly impacting the performance of the device or initiating an extortion-based attack.

In 2014, the U.S. Department of Homeland Security began investigating the security of medical devices. The findings from the Industrial Control System Cyber Emergency Response Team indicated that 300 devices from 40 different companies had hard-coded passwords. This design flaw, if unaddressed, gives hackers an open invitation to attack.

One type of threat that continues to plague even the highest-profile vendors is zero-day vulnerabilities. These software weaknesses are identified, exploited and often made public by cybercriminals without warning to the vendor. Older software can be targeted due to the lack of vendor patching support. However, newer software is just as vulnerable. Attackers are finding their way into recent software releases marketed as having advanced security defenses. In April 2015, more than 70 million websites

were at risk due to a remote code vulnerability affecting the Windows HTTP protocol. The following July, Microsoft issued one of its many emergency patches following an Italian surveillance software company's data breach and subsequent massive email leak. The hole was ultimately identified as a flaw in the Windows Adobe Type Manager Library through which cybercriminals could manipulate users into opening malicious files and website links.

FDA Regulations

Most manufacturers of medical devices are required to submit software updates and patches to the FDA for approval. This adds an extra layer of administration and regulation which can impact the timelines for those upgrades deemed critical to the functionality and safety of specific devices.

An Entire Universe of Older Connected Devices Currently in Use

In 2015, it was discovered that Hospira's Symbiq drug infusion pumps were at risk of being compromised through hospital networks. Specifically, the firmware configuration allowed hackers to alter the drug library on individual pumps, enabling potentially life-threatening alterations to drug dosages.

Network accessibility is only one threat to aging medical technologies that remain in use. The software is often not designed to accept patches or fixes if they are available; more frequently than not, upgrades are simply not developed. Additionally, reducing the risk in older implanted devices requires the mutual decision of patients and doctors to replace existing devices through surgery. Depending upon the health and stability of the patient, some device replacement procedures can be considered life threatening.

The Growing Malware Threat

What part of 'epidemic' is misunderstood? The number of malware samples discovered each year continues to reach record numbers with the latest estimates hovering around 300 million new strains detected in 2015. Trojans, potentially unwanted programs, ransomware, adware, spyware, worms, and viruses … they are all tools of the escalating cyberwarfare landscape.

It is virtually impossible for end-users of technology and IT management to keep pace with modern-day extortionists, blackmailers, and other manipulators of data security vulnerabilities by utilizing the legacy and flawed model of cybersecurity. Legacy antivirus and antimalware solutions that are based on signatures and heuristics are easily circumvented by today's malware.

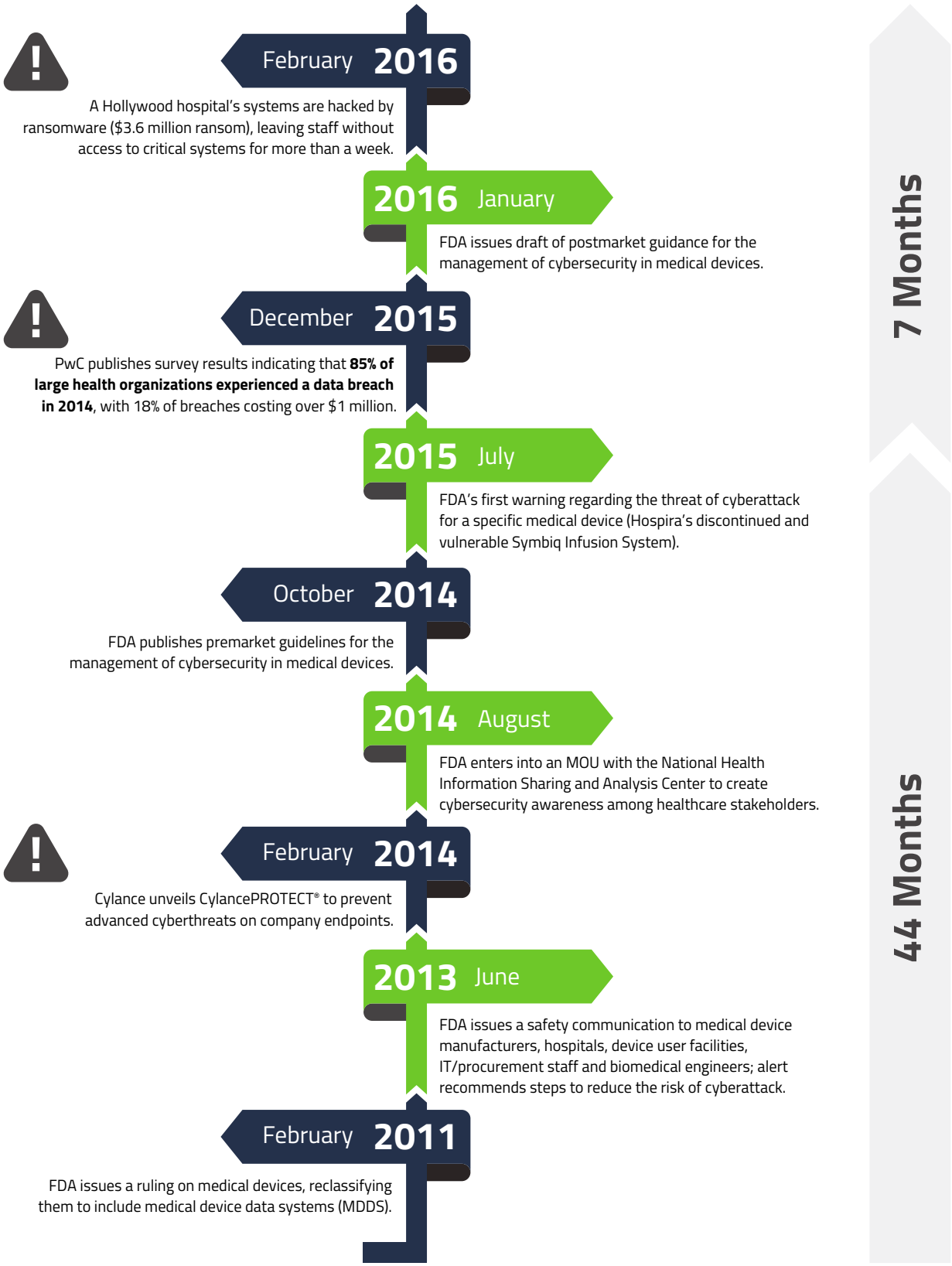
Malware today has advanced well beyond the days of the ILOVEYOU virus of 2000. Attacks today drop in stealth rootkits or malware that is mutating to avoid detection and often operating for months or years before being detected. The initial targets typically have softer defenses and are utilized to gain access to other systems that are data rich. Additionally, advanced social engineering techniques give cybercriminals a wider knowledge basis for threat opportunities and an increased threat surface to target with malicious code. A significant percentage of medical devices fit the target profile for endpoints that are vulnerable to cyberattacks.

Top 10 Healthcare Data Breaches 2015*

Organization	Records Breached	Type of Breach
Anthem Blue Cross Blue Shield	78,800,000	Hacking / IT Incident
Primera Blue Cross	11,000,000	Hacking / IT Incident
Excellus Blue Cross Blue Shield	10,000,000	Hacking / IT Incident
UCLA Health	4,500,000	Hacking / IT Incident
Medical Informatics Engineering	3,900,000	Hacking / IT Incident
CareFirst Blue Cross Blue Shield	1,100,000	Hacking / IT Incident
Department of Medical Assistance Services	697,586	Hacking / IT Incident
Georgia Department of Community Health	557,779	Hacking / IT Incident
Beacon Health Systems	306,789	Hacking / IT Incident

** From Forbes / Pharma & Healthcare 2015*

Timeline of FDA Response vs. State of Medical Device Security



FDA Regulations: Actionable Safeguards or Unfinished Business?

The timeline on page 4 illustrates the progression of the FDA's response to medical device cybersecurity over the past five years. Many agree that while this voluntary framework was an important place for healthcare providers and device manufacturers to begin addressing critical security gaps, current assessments reveal a weakening strategy incapable of addressing evolving and advancing threats from resourceful and potentially calculating cyberadversaries.

Traditional signature and heuristics-based protection fails to provide an effective defense as threats grow in sophistication (e.g. sandbox-aware malware). The FDA regulations are based on antiquated cybersecurity strategies and grossly underestimate the innovative capabilities of cybercriminals. The concept of an effective prevention security layer needs to be brought forth in order for the healthcare industry to right itself and deliver on the promise of administering quality care through uncompromised medical devices and hospital systems.

In a 2016 study published by the Institute for Critical Infrastructure Technology, researchers state that "in practically all matters of cybersecurity within the health sector, the FDA seems to be in a constant state of offering subtle suggestions where regulatory enforcement is needed... Due to the industry's continuous lack of cybersecurity hygiene, malicious EHR exfiltration and exploiting vulnerabilities in healthcare's IoT attack surface continue to be a profitable priority target for hackers."

FDA Premarket Guidelines for the Management of Cybersecurity in Medical Devices

1. Identify the device's intended use, security controls based on intended use, intent of interfaces, cybersecurity vulnerabilities
2. Protect:
   - Access through user authentication, physical locks, and strengthened password protection
   - Software and firmware updates with authorized authentication and user controls
3. Detect, Respond, and Recover
   - Implement features that allow for security compromises to be detected and acted upon
   - Develop and provide information to the end user concerning a cybersecurity threat
   - Implement device features that protect critical functionality
   - Provide methods for retention and recovery of device configuration by authenticated users

Management of Cybersecurity in Medical Devices

These programs should emphasize addressing vulnerabilities which may permit the unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient, and may impact patient safety.

Critical Components of a Postmarket Program:

- Monitoring cybersecurity information sources for detection of vulnerabilities and risk
- Understanding, assessing, and detecting presence and impact of a vulnerability
- Establishing and communicating processes for vulnerability intake and handling
- Clearly defining essential clinical performance to develop mitigations that protect, respond, and recover from the cybersecurity risk
- Adopting a coordinated disclosure policy/practice
- Deploying mitigations that address risk early

Growing Trends in Medical Device Vulnerability & Cybersecurity

The concepts of metamorphic and polymorphic malware are not new to those responsible for mitigating network and server exposure across industries. Yet, the impact of any disruptive malware attack — whether a system-halting Trojan or a ransomware payload — has become increasingly more costly.

- Since 2012, the number of victimized enterprises agreeing to make ransomware payment to hackers has increased 2.9% to 41% (Source: ISACA).
- In February 2016, the Hollywood Presbyterian Medical Center received another in a series of ongoing cyberattacks. Reports have indicated a possible $3.6 million ransom, the lack of access to critical care systems for more than a week, and the transfer of select patients to other hospitals.
- The CrytoWall v3 ransomware threat has cost users worldwide more than $325 million as they attempt to reclaim accessibility to their data.

A steady stream of eCrime adversaries enters the cyberthreat landscape daily, introducing new strains of file-encrypting malware. Spear-phishing activity continued to grow in 2015 with business email compromise (BEC) scams promoting hundreds of thousands of counterfeit websites and social engineering schemes tricking employees into divulging private information and transferring funds to fraudulent organizations.

In 2014, the director of emergency preparedness/operations and medical countermeasures for the FDA's Center for Devices and Radiological Health issued the following statement: "There is no such thing as a threat-proof medical device. It is important for medical device manufacturers to remain vigilant about cybersecurity and to appropriately protect patients from those risk."

Another growing trend in data and systems management — the booming migration of data outside of more traditional security platforms to public and hybrid cloud providers — has the attention of cybercriminals.

Volunteer groups and nonprofit cybersecurity advocacy groups began to surface in 2015 and 2016 with the intent of representing the interest of stakeholders in the areas of public safety. One group has gone so far as to update the language of the Hippocratic Oath to reflect, in their opinion, the dynamics of more modern healthcare practices and, specifically, necessary cybersecurity capabilities for healthcare providers.

There is a mounting responsibility placed upon healthcare providers and manufacturers to ensure the perpetual security and ongoing protection of medical devices despite, and in the midst of, frequent technological advancements. With or without regulatory mandates, the responsibility falls upon IT teams and product design specialists to close the gaps on risks to patient safety.

Cylance: Solutions for Every Step in the Kill Chain

All cyberattacks are planned and delivered in nearly the same manner, seldom straying from a high-level process map known as the 'Cyber Kill Chain.' The only variable is the amount of resources cybercriminals spend on the different stages of an attack. No matter where your problem lies on the cyberattack spectrum, Cylance stops malicious files before they can execute.

What Makes Cylance Different?

Most endpoint protection platform (EPP) providers are seeking to do one thing: remediate a threat. The concept of remediation implies one important consideration — the reality that a threat has already taken place. Certainly, there are impressive dashboards designed to help hospital IT managers and device manufacturers control active cybersecurity events. However, they do not take into consideration several critical dynamics within the healthcare industry:

- A remediation-dependent system relies upon the management of highly trained IT professionals who can monitor and respond on a 24/7 basis. This can be a challenge for resource-constrained support organizations.
- Valuable time is lost and financial resources consumed while system analysts research events and follow protocols to remediate.
- Zero-day vulnerabilities often go unaddressed.

In February 2016, Gartner, Inc., reported that by 2018, 60% of EPPs will restrict executables that have not been preinspected for security and privacy risks, up from 22%. The stage has been set for those providers innovating with disruptive solutions that can detect a growing number of variant threats before they happen while minimizing the endpoint and network IT management requirement.

Utilizing a revolutionary artificial intelligence agent, Cylance's products and services are designed to proactively prevent the execution of advanced persistent threats and malware.

Key Product and Service Strengths

- Proactively detects new variants and repacked versions of existing malware.
- Delivers a minimal impact on networks and endpoints (continues to work with less than 1% of CPU memory and loss of Internet connectivity).
- Offers a cloud-based management console without the requirement of cloud-based detection.
- Generates static file assessment reporting for learning across customers and quarantines.
- Reach expands to OEMs who can utilize our solutions to secure embedded systems and medical devices.
- Supports Windows and Mac devices; Linux available soon.

Industry Response

Gartner recognized Cylance as a Visionary in its 2016 EPP Magic Quadrant. Cylance believes this is because we are one of the fastest-growing companies in the history of cybersecurity and provide an innovative new approach that replaces legacy signatures found in legacy antivirus products.

Cylance technology is currently deployed on over six million endpoints and protects hundreds of enterprise clients worldwide, including Fortune 100 organizations and government institutions.

Take the Next Step

To begin a discussion or for further information on applying artificial intelligence, algorithmic science, and machine learning to cybersecurity, please contact:

Rob Bathurst
Managing Director, Healthcare and Life Sciences
Email: rbathurst@cylance.com
Phone: +1-877-973-3336

Important Links

Postmarket Management of Cybersecurity in Medical Devices: http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communications http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm

Content for Premarket Submissions for Management of Cybersecurity in Medical Devices http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

2016 Gartner EPP Magic Quadrant Report https://www.cylance.com/gartner

Contact Information

Visit www.cylance.com/criticalinfrastructure to learn more.

https://www.youtube.com/user/CylanceInc

https://www.linkedin.com/company/cylanceinc

https://www.facebook.com/CylanceInc

https://twitter.com/cylanceinc

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612