COSMOS
Navigate the Compliance Universe

Compliance Today - January 2020
Compliance-driven risk reduction strategies for medical devices

By Clyde Hewitt and Cory Blacketer

Clyde Hewitt (clyde.hewitt@cynergistek.com) is Executive Advisor and **Cory Blacketer** (coryn.blacketer@cynergistek.com) is Medical Device Security Consultant at CynergisTek, headquartered in Austin, TX.

Three simple steps will focus light on why medical devices are a compliance problem:

- Step 1: Obtain a copy of the "Could Not Locate" (CNL) list from the director of your clinical engineering department. The CNL list identifies all medical equipment that missed prior preventive maintenance actions, and is required by the Joint Commission, Standard 6.20.[1]
- Step 2: Do research to determine which medical device(s) identified in the CNL list can potentially create, store, or access protected health information (PHI). It is not necessary that the device be currently connected to the provider's network.
- Step 3: Ask if your organization has evaluated all missing devices in the filtered list from Step 2 to see how many patients may have had their data compromised. Remember that under the HIPAA Omnibus Rule, organizations must start with a presumption of breach. If no breach has been reported, a "low probability of compromise" analysis should be documented in your files.

What is the problem?

Every day in the United States, a physician relies on advanced medical technology to help diagnose the cause of their patients' life-threatening conditions. If the visual clues indicate a stroke, including slurred speech, numbness, or weakness in limbs, and facial weakness (especially on one side), then time is critical. Strokes can be caused by either internal bleeding or a blood clot in the brain. Without advanced medical technology to diagnose what is not outwardly visible, the wrong treatment (e.g., blood thinners) is very risky and can result in a long-term disability or even death.

Medical devices are an invaluable tool to help make the correct diagnosis, but at some point, we will experience situations where these advanced medical devices are not available when needed due to malware or ransomware. As of August 2019, 82% of healthcare organizations, Internet of Things (IoT) manufacturers, and other organizations that use IoT devices have faced a cyberattack focused on IoT within the last 12 months, as identified by security firm Irdeto and reported in *HealthITSecurity.com*.[2] The trend is disturbing, because just 18% of healthcare providers reported an attack on their medical devices in October 2018.[3]

The significant increase in numbers of attacks represents a clear escalation of the threat. The results are an increased risk to patient safety, clinical outcomes, service disruptions, and loss of patient data leading to compliance issues. To counter this threat, providers have increased both the number of people and the amount of financial resources to address the adverse impacts; however, we continue to experience a significant increase in attacks. Exploring the causes of this increase in cyberattacks is not difficult; more than 76% of healthcare providers responding to the 2018 KLAS[4] Survey said a lack of resources limited their security capabilities.

"Just fix it!" is easier said than done

Hospitals that recognize the security and compliance challenges still struggle to develop a strategy to close the gaps. Security compliance metrics[5] collected by CynergisTek suggest that, although there has been some progress addressing the security of traditional IT systems like workstations and servers since 2018, the majority of healthcare organizations still fall short of the minimum expectations for even their basic security needs. The fact that medical devices lag even more is understandable when one examines the root causes.

Medical devices have more vulnerabilities than traditional IT-managed workstations and servers. The reasons vary, but the primary reason is that device manufacturers were never held accountable for the security of their products before the Food and Drug Administration (FDA) first published the Pre-Market Guidance in 2014. The FDA continues to revise the guidance and has taken a more aggressive approach to ensuring the cybersecurity of medical devices.[6] The latest draft was dated October 18, 2018.

The unintended consequences of aging equipment

Without accountability, we see that medical devices have an unusually long life cycle when compared to other IT systems. It is very common to see medical devices in service for more than 15 years, especially considering the high investment. This long life cycle means that the underlying operating system was likely "new" between 15–20 years ago. When we examine these medical devices, we find them running Microsoft Windows 98, 2000, or 2003—all of which are past their end of life and are no longer supported by the vendor. Devices designed 15–20 years ago were generally not designed to be upgraded or patched and have limited memory or onboard storage. Hackers are aware of this, and vulnerabilities corrected decades ago with new operating systems remain in the legacy devices.

Older medical equipment was also never intended to use anti-virus software. End-point protection software, something ubiquitous to every workstation, can't be used to protect medical devices. Although encryption is used to protect workstations and is the foundation of a "safe harbor" defense, medical devices that contain patient data cannot benefit from the same technology. Hospitals that experience lost or stolen devices containing patient data must presume they have experienced a breach of patient confidentiality. Only recently have we seen medical device manufacturers include encryption as an option, but even then, safe harbor cannot be proven if generic user IDs and access controls are used.

Hospitals that still use medical devices acquired in 2006 may find that those devices rely on legacy systems and insecure Wired Equivalent Privacy (WEP), a security protocol used in wireless networks,[7] which required the use of a single shared "key" to connect. In order to keep those devices operational, those hospitals must manage a separate WEP wireless network, resulting in a very high risk that a hacker can compromise the network and, ultimately, the entire hospital. Once a legacy medical device is compromised, those vulnerabilities allow medical devices to be susceptible to a variety of malware that is in a hospital. Other systems may not be vulnerable, but medical devices cannot only be affected but serve as the "index" device that will continually re-infect other vulnerable systems as they are brought online.

Finally, with more than 10,000 medical device manufacturers, hospitals find themselves struggling to develop and maintain an accurate inventory, but more importantly, knowing what operating system is being used and what vulnerabilities exist. As Dr. Christian Dameff, cybersecurity researcher and informatics fellow at the University of California San Diego Health, stated,[8] "When WannaCry hit, hospitals were scrambling to figure out which medical devices were impacted. These devices are often black boxes to hospitals."

These additional challenges are holding the medical device community back from achieving the compliance levels of other traditional workstations and servers in the IT department.