The Danger of Being Connected

Save to myBoK

By Ty Greenhalgh, HCISPP

In 2014, the American Recovery and Reinvestment Act required and incented hospitals to demonstrate "meaningful use" of an electronic health record (EHR). Hospitals, desiring to maintain existing Medicaid and Medicare reimbursement levels and avoid penalties, spurred a rapid digitization of medical records. Unwittingly, they also created an irresistible incentive for hackers.

In 2015, practitioners recognized the value of networking medical device data directly into the EHR, which could reduce errors, increase real-time documentation, and improve workflow. While these connected medical devices resulted in numerous new benefits, they also increased the risks to compliance and patient safety. To prevent harm to patients and to protect a hospital's assets, understanding the threat and understanding strategies for an effective response is imperative. This article covers the scope of current threats and resources for providers.

Medical Device Vulnerabilities

A 2017 Ponemon[1] study of anonymous respondents, "Medical Device Security: An Industry Under Attack and Unprepared to Defend," found 44 percent of hospitals had experienced an attack on a medical device that resulted in adverse events or harm. Inappropriate treatment was the outcome in 38 percent of the events. Patient beds alone have an average of 14 medical devices that can be connected, built in, or incorporated into their design.

In addition to fighting escalating cyberattacks, healthcare privacy and security professionals are also focused on meeting regulatory compliance for the confidentiality of electronic protected health information (ePHI). They also are now realizing that compromising the integrity of data or the availability of systems will adversely impact patient care. Medical device risk management is now evolving to address all three areas of the CIA Information Security Triad: Confidentiality, Integrity, and Availability.

Emergency room doctors rely heavily on a CT scanner's availability and integrity to quickly diagnose stroke patients and determine if a stroke is hemorrhagic or ischemic. A delayed diagnosis could easily result in loss of motor functions, brain damage, or even death.

Besides medical devices, major healthcare systems possess tens of thousands of networked devices that are part of what is often referred to as the Internet of things (IoT) and operational technology (OT) devices. These devices can be elevators, HVAC units, video conferencing equipment, printers, and blood refrigerators, all of which are critical to patient care and—like medical devices—extremely vulnerable to cyberattacks. In addition to being directly compromised, medical, IoT, and OT devices can be used as a hacker's entry point into the hospital network, putting patient safety, ePHI, billing records, and intellectual property at risk.

A recent industry-wide survey from ZK Research[2] found that a disturbing 61 percent of network professionals have little confidence they know what devices are connected. Many IT departments believe the same security tools used to protect general network infrastructure can secure healthcare environments. However, unlike other IT endpoints, connected medical, IoT, and OT devices are hardly visible in native IT control systems. This puts non-healthcare-focused security solutions at a profound disadvantage.

Network access control (NAC) systems are commonly used to manage traditional endpoint devices such as servers, desktops, laptops, and portables. Traditional NAC takes a broad view of the network. However, most NACs provide inadequate contextual information about medical and IoT device use, traffic flows, or operational status, which would render an administrator, for example, unable to determine why one Baxter infusion pump is communicating with North Korea while the other 999 pumps are not. Typically, NAC cannot see the IP or networking information, which reveals the true nature of a device and the context of its communications within the network. A NAC's inability to distinguish medical devices often fails to identify MRI machines and instead classifies them as unknown devices.

This poor device visibility results in system administrators continuously mixing unknown vulnerable devices into network segments without thought to the National Vulnerability Database's recommendations on mitigating their risk. Because these devices were never designed to support an authentication certificate, system administrators simply configure a NAC bypass allowing the unknown devices' automatic authentication. The solution isn't as simple as restricting access. These devices are incredibly sensitive to vulnerability scans and blocking these devices is not an option as it may interrupt practitioners administering patient care. A key medical device management maxim is "Don't inadvertently shut off the device administering life-saving medication to the patient."

High Profile System Vulnerability Events

In recent years, several incidents and compromised devices have threatened patient care. A few examples include:

1. BlueKeep, a self-replicating malware worm that exploits Microsoft's Remote Desktop Protocol (RDP) and allows bad actors to remotely access and control the endpoint. In May 2019 Siemens reported vulnerabilities in several medical devices that could be exploited by BlueKeep. The severity of these vulnerabilities are rated a 9.8 out of 10 on the MITRE's Common Vulnerability Score System (CVSS). ECRI, a federal patient safety organization, forecasted RDP as the top healthcare technology threat for 2019. Many medical devices, including critical radiology devices, run legacy Microsoft Windows operating systems, making them likely targets to hackers and indiscriminate malware.
2. Becton Dickinson's Alaris Gateway Workstation (AGW) provides power and network connectivity to infusion and syringe pumps. An improper access control vulnerability allows hackers to remotely upload malicious firmware to infusion pumps, causing them to dispense all the patient's medication in minutes instead of hours. During the 2019 RSA Conference, doctors simulated the emergency on stage. In June 2019, the FDA recalled Medtronic's MiniMed pump for this vulnerability. The United States Department of Homeland Security's advisory on the AGW has a CVSS rating of 10 out of 10.
3. At Israel Deaconess Radiology System, a network tech connected to the internet for a firmware upgrade and went to lunch.[3] Malware was downloaded and 2,000 X-ray images were stolen. According to media reports, the X-rays were sold to Chinese nationals with lung diseases who wanted to travel outside the country for treatment.

Suspicious Activities Worth Monitoring

1. All unpatched devices vulnerable to the BlueKeep virus are not quarantined.
2. The elevator control system is trying to communicate with a human resources application.
3. Ninety-three percent of your IP-based security cameras are using default passwords and security configurations.
4. You're considering contacting the US Department of Health and Human Services' (HHS) Office for Civil Rights because 20 devices on the "gone missing" list are not using data encryption.
5. It's unclear which medical devices are running Windows 7, which will be discontinued in January 2020.

6. Heart monitors recalled by the FDA are still in use.
7. A CT scanner is sending payment card industry data to an IP address in Ukraine.

The CHIME CEO and the Association for Executives in Healthcare Information Security (AEHIS) chair recently wrote[4] to Senator Mark Warner (D-VA), an author of the 2015 Cybersecurity Act (CSA). Under Section 405, the CSA requires the Secretary of HHS to address improvements for cybersecurity in the healthcare industry. They voiced their support for several FDA policy proposals, including the draft guidance that will address the "serious threats to patient safety stemming from cybersecurity threats to medical devices." Their letter covered eight primary points, including the following five, which specifically address medical devices:

1. Regulators need to understand medical device risks extend to the entire network, thus posing a real risk to patient safety.
2. The FDA should expand the definition of medical device risk to include networks, switches, firewalls, applications, and other components.
3. Global WannaCry 2017 patches have not been released for certain medical devices.
4. Medical device manufacturers need certification standards similar to EHRs.
5. The FDA's premarket guidance on medical devices should explicitly reference the voluntary guidance provided by HHS, in response to the CSA Section 405 mandate "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients," to serve as a resource to improve their cybersecurity posture.

The HHS voluntary guidance publication, described in the preceding list in item five, identifies medical devices as one of the top five cybersecurity threats to the healthcare industry. Offering practical solutions for small, medium, and large organizations, the guidance can be downloaded from the Public Health Emergency website.

Fortunately, within the last year, solutions designed specifically for medical and IoT device security have appeared on the market. These systems leverage automated and intuitive technology to passively scan the network without disrupting the devices or network activity, then parse the network metadata to automatically classify, manage, and safeguard all the devices.

This new visibility into device inventory and communications promises health systems the ability to apply sophisticated machine learning to accurately classify each device and leverage artificial intelligence to baseline its dynamic behavior within the context of a provider network. This additional level of detail should permit clinical engineers and chief information security officers to engage the IT department in defining and implementing actionable policies that significantly reduce exposure to patient harm and regulatory noncompliance.

Healthcare organizations like CHIME and AEHIS have discovered that patient safety risks attributed to medical devices are not contained to the device itself. These risks extend to the network, firewalls, switches, and operating systems. Healthcare delivery organizations are recognizing that medical, IoT, and OT device privacy and security are components of enterprise cyber and privacy risk management. A holistic approach is the only reliable way to deliver closed-loop security for patient safety and critical assets in our hyper-connected healthcare enterprise.

Notes

1. Ponemon Institute. "Medical Device Security: An Industry Under Attack and Unprepared to Defend." https://www.synopsys.com/software-integrity/resources/analyst-reports/medical-device-security-report.html.
2. Kerravala, Zeus. "IoT Security Plans: 3 Things You Must Include." *Network World*, February 27, 2010. https://www.networkworld.com/article/3343184/protecting-the-iot-3-things-you-must-include-in-an-iot-security-plan.html.

3. Roberts, Paul. "What's the Value of a Stolen Chest X-Ray? More Than You'd Think." *Data Insider*. January 26, 2017. https://digitalguardian.com/blog/whats-value-stolen-chest-x-ray-more-youd-think.
4. The College of Health Information Management Executives and the Association for Executives in Healthcare Information Security letter to Sen. Mark Warner, March 22, 2019. https://chimecentral.org/wp-content/uploads/2019/03/CHIME-AEHIS-Warner-Response-vFINAL.pdf.

Ty Greenhalgh (Ty@CyberTygr.com) is the managing principal and founder of Cyber Tygr.

Article citation:
AHIMA. "The Danger of Being Connected" *Journal of AHIMA* 90, no.8 (August 2019): 38-39, 55.