Expert Insights

—

Medical devices are vital, but vulnerable

Treat infrastructure risks to safeguard patient care

IBM **Institute for Business Value**

IBM

Experts on this topic

Beth Musumeci

Global Partner,
IBM Security Services,
Healthcare and Life Sciences
linkedin.com/in/beth-musumeci-97550a3/
beth.musumeci@ibm.com

Charged with empowering customers with innovative security solutions, Beth Musumeci has more than 20 years of experience in cybersecurity work for the private sector and for the US federal government. She was an early pioneer in establishing security operations centers and global logical security operations.

Ralph Ramsey

Associate Partner,
IBM Security Services,
Healthcare and Life Sciences
linkedin.com/in/ralphramsey/
ralph.ramsey@ibm.com

Ralph Ramsey is a diversified technologist and practitioner with 25 years' experience in network communication and cybersecurity. He led security initiatives for the US Defense Information Systems Agency (DISA) and Mass Transit Authority of New York City (MTA), and as key advisor in IoT, endpoint security, and intrusion prevention and detection for tech-startups. Ralph currently provides clinical cybersecurity consultation for healthcare providers, government agencies, and manufacturers.

Stephen Brennan

Global Associate Partner,
IBM Security Services,
Healthcare and Life Sciences
linkedin.com/in/stephenslogic/
stephen.brennan@ibm.com

Stephen Brennan is a recognized cybersecurity and technology global leader with over 20 years of strategic and technical leadership and innovation experience. This includes developing and protecting critical national and operational infrastructure, data, and systems. Stephen works with industry leaders to understand evolving threats and risks to patient safety, security, and privacy and to explore opportunities that enhance patient outcomes.

Smart technologies and streaming data are remaking both provider-to-patient clinical devices and business-to-health consumer wearables.

Talking points

Medical device security is a big problem, and an old one

Older medical devices weren't designed with cybersecurity as a forethought, and are hard to properly secure. Now the boom in newly connected devices is exposing pre-existing vulnerabilities.

Health systems need to prioritize, and invest in, cybersecurity

Enveloping legacy and newer devices with end-to-end protection assures they're being used properly and for their intended purposes.

Deliver intended outcomes despite adverse cyber events

From cyber resilience to cyber wellness, securing medical devices can help prevent operational disruption and protect patient safety and privacy.

—

Treating healthcare cybersecurity woes

In current hospital systems, many devices are old, hard to see, and unprotected from vulnerabilities and hacking. Legacy medical devices were never designed to be connected—let alone secured—on today's digital networks. Yet they hold sensitive, personal, and often times life sustaining information. Supporting medical needs ranging from a seemingly benign saline drip, to radiation targeting systems, continuous sedation during surgery, and recovery diets to eat at home after discharge, medical devices are closest to patients, second only to their primary care physicians.

Medical devices pose a unique cybersecurity risk in that attacks or hacks can directly endanger patient privacy and safety. What makes medical device security such a pressing issue are the network effects associated with connected platforms. Compromising the safety and wellness of one individual is problematic enough, but these vulnerabilities expose entire segments of patients and consumers using specific devices, applications, and services.

Emerging technologies, however can identify medical devices, understand their vulnerabilities, and provide non-intrusive security on the network.

Connected consumers, disconnected devices

A subset of the Internet of Things (IoT), the Internet of Healthcare Things (IoHT) is the convergence and integration of sensor data collected by medical devices and mobile technologies, as applied to healthcare.[1] Devices linked to cloud platforms on which captured data is stored and analyzed has come to be known as the Internet of Medical Things (IoMT).[2]

FDA: Suite of network bugs identified[3]

The US Food and Drug Administration (FDA) was made aware of 11 cybersecurity vulnerabilities that, if exploited by a remote attacker, could put critical medical devices and networks at risk. A suite of network protocol bugs, URGENT/11, as it's called, illustrates the problem of unmanaged embedded devices.

Insight: Insulin pump vulnerable to hacking[4]

In 2016, a computer security firm revealed a vulnerability in an insulin pump manufactured by a global medical device maker that could allow a hacker to take control of it and dose from a distance of up to 25 feet. There were no reported attacks.

Insight: Bring your devices to work day[5]

Nearly three-quarters of hospitals have a "bring your own device" (BYOD) policy that lets staff use personal computers, smartphones, and other devices for work purposes.

The healthcare consumer movement to participate in wellness rather than treatment—or value-based health—is one factor driving the adoption of new medical technology, a shift that started when personal activity trackers and wireless-enabled wearable technology devices became wildly popular.[6] But devices connected to cloud apps run the risk of exposing health networks to malware and other attacks.

Adding to the broader challenge of connected devices, manufacturers have little incentive to secure devices for the full lifecycle and instead outsource device support and maintenance (see sidebar, "FDA: Suite of network bugs identified").

Ensuring integrity across the device lifecycle starts with manufacturers. Security is about integrating the supply chain from design to end of life of the device. Data management, product and service maintenance and support should be considered essential features of any device.

Consider the scale

There are 10 to 15 million medical devices in US hospitals, and an average of 10 to 15 connected devices per patient bed.[7] Multiplied by the hundreds of thousands of hospital beds nationwide,[8] the magnitude becomes clear. The number of global connected medical devices is set to exceed 50 billion in the next decade.[9] And that's not just inside hospitals, as doctors treat patients via virtual medicine and consumer wearables send data to clinicians.

Especially jarring is that 82 percent of healthcare organizations have experienced an IoT-focused cyber attack in the last year, but only 6 percent say they have the resources to tackle cybersecurity challenges.[10]

Cybersecurity for healthcare should be borderless, extending to the safety of patients admitted and those at home.

There's more at stake than privacy

Healthcare systems are easily overwhelmed by the challenges of securing devices and making them visible on the network. In many cases that's because they're trying to administer endpoint devices not designed for easy administration—namely security hygiene capabilities like visibility, analytics, patching, and remote administration.

What matters most is the well-being of the patient, but that's increasingly dependent on the integrity of data from a vulnerable piece of equipment or an unsecured medical device. Top of mind for caregivers is anything that constitutes a risk to patient safety, such as changing a diagnosis or the prescribed dosing schedule from an automated insulin pump (see sidebar on page 2, "Insulin pump vulnerable to hacking"). For critical conditions, device and data integrity can mean the difference between life and death.

Securing medical devices isn't just a concern for individual patients, providers, or healthcare systems. Access to care and care delivery services could be considered components of critical infrastructure. Medical sabotage could threaten national and international governance from the top down. Thirteen years ago, the heart defibrillator of then US Vice President Dick Cheney was modified so it couldn't be hacked.[11] The infrastructure of healthcare, too, must be protected from odious or retaliatory action, for example shutting down or obliterating an entire online electronic medical record system.

While such examples may be exceptional, they illustrate the unforeseen consequences of embedded, connected devices. The integrity of medical devices and personal information serves a larger societal need. Healthcare connects people of all backgrounds, from every part of the world. It touches the lives of everyone.

The time for change

Unique security challenges exist in clinical settings since typical performance indicators like confidentiality, integrity and availability aren't the primary focus. Security approaches and outcomes focus on up-time and reliability (see Figure 1). Patient safety, of course, is the ultimate outcome.

Hospitals and care delivery centers are especially vulnerable. The care delivery environment is now a continuously changing mix of in-house medical devices, connected IoMT devices, and BYOD wearables, not to mention the applications and services that operate on these devices. Nearly half of large data breaches in healthcare can be attributed to theft and loss,[12] yet three-out-of-five physicians use personal devices for work, even when BYOD isn't allowed (see sidebar on page 2, "Bring your devices to work day").[13] Any connected device has the potential to compromise the broader IT network. For example, consumer self-service portals offer patients the ease and convenience of digital access to their health records, but also increase risk of data breach and attacks from malware, ransomware, and phishing.

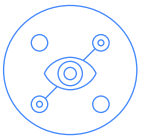
Figure 1

Security complexities within hospital environments are unique

Security approaches and outcomes focus on up-time and reliability

Risks

- Lack of risk mitigation and remediation
- Hard to test production environments
- Limited security awareness
- Disparate IT and medical information teams
- Limited patching



Visibility

- Limited asset visibility
- Seeing all devices across departments and units is critical
- Operational data and security analytics visibility is limited

Impact

- Security incident impact can be catastrophic
- Lack of a security incident response plan and playbook can create significant business disruption

Source: IBM Security.

In the life and death environment of emergency care delivery, device downtime is often not possible. Such environments are characterized by constant data from information technology, operational technology, and biomedical devices. Whether due to budget and capacity constraints, skills gaps, or complexity, these networks are often fractured and vulnerable. Often, these vulnerabilities reflect underlying problems in technology and security governance. Many hospitals are unprepared to prioritize security because they've not assessed current risk and, as a result, don't have effective security policies.

Consider the complexity associated with providing a resilient, cybersecure care delivery environment: Connecting and securing different vendors and their devices, a continuously changing mix of patients and staff, and myriad exchanges of data across the healthcare supply chain. This complexity, especially when combined with the speed of data and decision-making in critical care situations, presents a unique risk to every provider. Given the consequences of failing to secure the care delivery environment, these risks must be assessed and prioritized.

Just as the goal of healthcare is wellness and prevention, the goal of cybersecurity is resilience and avoidance. Information sharing in a hyper-connected environment is the new reality, and device and data security critical for device manufacturers, care providers, and health consumers.

Similar to healthcare, cybersecurity resilience is a result of prevention, hygiene, and wellness.

Face the uncertainty

As connected medical devices spread exponentially, healthcare providers are greatly challenged to protect patients both medically and in cyberspace. Many are turning to IT vendors for guidance and insight into the technologies that can help improve information security and patient safety. We suggest focusing on three areas to foster cyber resilience:

Strategy and risk. Healthcare security is uniquely challenging given the reliance on technology platforms and the consequences associated with errors and vulnerabilities. Unify departments, functions, and partners across your network via shared risk management and security governance frameworks. Strategy and planning, risk assessment, and information sharing should reflect continuous collaboration and mutual accountability.

Threat management. Integrate your operational development, delivery, and support capabilities so they see across boundaries of information technology, operational technology, and partner/ provider technology. Detect and stop advanced threats targeting medical devices and their supporting infrastructure. Better still, avoid vulnerabilities in the first place by integrating security into care design and delivery and investing in prevention and maintenance to promote cyber hygiene, wellness, and resilience.

Digital trust. Protect critical assets, such as health records and sensitive personal information that's connected to medical devices. Govern users and identities to enhance digital trust. Help ensure that your application, platform, and cloud service providers understand their shared responsibility for cybersecurity performance and resilience. Most importantly, unify endpoint management so there's greater visibility of devices across the network.

Action guide

Medical devices are vital, but vulnerable

1. Diligently manage user access

Protected health information makes providers a primary target for malware, crypto jacking, phishing, and other security threats. Know who's been granted entitlements to access sensitive functions or data, and monitor and audit actions of privileged users closely.

2. Assess and address device vulnerabilities

Evaluate the medical device landscape and prioritize adoption and investment in products that are both more secure and that address existing vulnerabilities.

3. Improve your security maturity across the care delivery ecosystem

Update security strategies that align practices with broader risk frameworks. Make security an essential part of the care delivery lifecycle, from planning to operational and support processes. Make security a shared responsibility by communicating and collaborating with consumers, first-, second-, and third-party providers.

Notes and sources

1 Winey, Todd. "IoT in Healthcare Is Really the Internet of Patients (IoP)." *Healthcare IT News*. January 2017. https://www.healthcareitnews.com/sponsored-content/iot-healthcare-really-internet-patients-iop

2 Rouse, Margaret. "IoMT (Internet of Medical Things) or healthcare IoT." IoT Agenda. August 2015. https://internetofthingsagenda.techtarget.com/definition/IoMT-Internet-of-Medical-Things\

3 "URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices." FDA. October 2019. https://www.fda.gov/medical-devices/safety-communications/urgent11-cybersecurity-vulnerabilities-widely-used-third-party-software-component-may-introduce

4 Doheny, Kathleen. "How Hackable is the One Touch Ping Pump?" EndocrineWeb. March 2019. https://www.endocrineweb.com/news/diabetes/55330-how-hackable-one-touch-ping-pump

5 Chapple, Mike. "5 Strategies for Implementing a BYOD Policy in Healthcare." *HealthTech Magazine*. September 2019. https://healthtechmagazine.net/article/2019/09/5-strategies-implementing-byod-policy-healthcare

6 Jain, Anil, M.D., Anita Nair-Hartman, Heather Fraser, and Sanjeev Saravanakumar. "The emergence of value-based health." IBM Institute for Business Value. November 2019. https://www.ibm.com/downloads/cas/N2NNWYXG

7 Landi, Heather. "82% of healthcare organizations have experienced an IoT-focused cyberattack, survey finds." Fierce Healthcare. August 2019. https://www.fiercehealthcare.com/tech/82-healthcare-organizations-have-experienced-iot-focused-cyber-attack-survey-finds

8 "How Many Hospitals Are in the US?" Definitive Healthcare. February 2019. https://blog.definitivehc.com/how-many-hospitals-are-in-the-us

9 "Guide To The Connected Healthcare Device Market and Growing Market Share." Linchpin. December 2019. https://linchpinseo.com/guide-to-connected-healthcare-device-market/

10 "New Report Reveals Vulnerabilities of Internet of Things-enabled Healthcare Devices." ITN Online. August 2019. https://www.itnonline.com/content/new-report-reveals-vulnerabilities-internet-things-enabled-healthcare-devices

11 "How Dick Cheney Protected His Defibrillator from Terrorists." MDDI Online. October 2013. https://www.mddionline.com/how-dick-cheney-protected-his-defibrillator-terrorists

12. "To BYOD or not to BYOD: the benefits and risks." Health Management. January 2018. https://healthmanagement.org/c/hospital/news/to-byod-or-not-to-byod-the-benefits-and-risks

13 "10 Facts About BYOD." 2018. Spok. https://www.spok.com/infographic/infographic-byod/

About Expert Insights

Expert Insights represent the opinions of thought leaders on newsworthy business and related technology topics. They are based upon conversations with leading subject matter experts from around the globe. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
March 2020