Search   🔍   *or* BROWSE BY TOPIC

CONTACT US

hfma™

JOIN

MEMBERSHIP   EDUCATION   PUBLICATIONS   FORUMS   CAREERS   MARKETPLACE   INDUSTRY INITIATIVES

HFM MAGAZINE: JULY 2017   HFM   ARCHIVES   SUBMIT ARTICLE

ADVERTISING & SPONSORSHIPS   REPRINTS   SUBSCRIBE

Cybersecurity and the Internet of Things

DANIEL R. VERDON

◄ 1

The opportunity to improve health through technology comes with risk. With increasing cybersecurity attacks to our nation's infrastructure, health care faces a growing threat from the very technology that also creates a life-saving potential.

It was not long ago that healthcare leaders' primary technology focus was on protecting health information and thwarting data breaches. Indeed, these issues continue to be a priority, with 2016 having been declared the most active year yet for data breaches by the Department of Health & Human Services' Office for Civil Rights. But the explosive growth of the Internet of Things (IoT)—i.e., the interconnected computing power of myriad devices—poses even greater risks.

In February 2017, Gartner, a research and consulting firm based in Stamford, Conn., estimated that 8.4 billion connected devices were would be in use worldwide in 2017. And the numbers are expected to grow exponentially. In 2013, Cisco predicted the number of connected devices would mushroom to 50 billion by 2020. That number was modified down in 2014 by McKinsey & Company, which predicted there will be closer to 20 billion to 30 billion devices during the same time period. By 2025, McKinsey predicts that health care will account for one-third of the market for IoT connected devices.

Such growth of technology, computing power, and the interconnectedness of devices not only is creating tremendous opportunity but also poses a large-scale risk for healthcare providers.

Our healthcare technology infrastructure is not adequately prepared for this growth. A June 2017 report by the Health Care Industry Cybersecurity Task Force states that the country's cybersecurity infrastructure is actually in critical condition.

"Our nation must find a way to prevent our patients from being forced to choose between connectivity and security," the report states.

The problems are multifactorial, complex, and expensive. Most healthcare organizations face substantial resource constraints, the report says. "[B]oth large and small healthcare delivery organizations struggle with numerous unsupported legacy systems that cannot easily be replaced (hardware, software, and operating systems) with large numbers of vulnerabilities and few modern countermeasures."

The report recommends six tactics to improve healthcare's cybersecurity:

- Define and streamline leadership, governance, and expectations for healthcare industry cybersecurity.
- Increase the security and resilience of medical devices and health information technology.
- Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
- Increase health care industry readiness through improved cybersecurity awareness and education.
- Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure.
- Improve information sharing of industry threats, weaknesses, and mitigations.

The report states, "Over the next few years, most machinery and technology involved in patient care will connect to the Internet; however, a majority of this equipment was not originally intended to be Internet accessible, nor designed to resist cyber attacks."

The message for healthcare leaders is that technology can truly transform patient care, yet one of the greatest challenges in the near-term will be to build a healthcare digital infrastructure that can use the National Institute of Standards and Technology Cybersecurity Framework to identify, protect, detect, respond, and recover, and adopt and use technology that can help facilitate high-quality care for patients in need.

Publication Date: Wednesday, July 05, 2017