HIT Think Why the explosion of IoMT exposes providers' security weaknesses

By **Barry P. Chaiken**
Published June 16 2016, 5:32pm EDT

More in **Cybersecurity, Hacking**

While a majority of consumers use their Fitbits, Apple Watches and other activity trackers for a period of only three months before abandoning them, many healthcare providers see promise in using the data generated from these devices to more closely manage care outside of the physician's office.

In addition, inexpensive yet sophisticated newly developed medical sensors are regularly offering care providers innovative and exciting ways to collect medical data on patients to help manage care and monitor health. These devices use Bluetooth, Wi-Fi or RFID technology to connect to the Internet and transmit data to a variety of healthcare information technology tools, such as electronic medical record systems and population health databases.

These Internet of Medical Things (IoMT) form a subset of the larger Internet of Things (IoT) universe, which has been pursued aggressively in other industries to make machines "smarter" by enabling them to communicate and coordinate with one other.

With exposure to the Internet comes risk of hacking, viruses, malware and ransomware. Last year, two security researchers demonstrated how to disable the transmission of a hacked 2014 Jeep Cherokee. This demonstration led Chrysler to recall 1.4 million vehicles and send owners a USB drive to update the car's software. In response to this and other events, the FBI,

Department of Transportation and the National Highway Traffic and Safety Administration issued warnings to the public to take steps to protect the software integrity of their vehicles.

Although no credible reports exist showing the hacking of medical equipment in an effort to harm patients, the risk exists and worries cybersecurity experts. Previous medical device hacks focused on stealing patient information for financial gain (for example, banking information), but experts demonstrated hacks that adjusted medication doses in infusion pumps, surely a potential harm to patients.

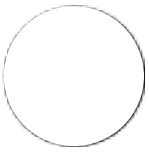
Earlier this year, unknown hackers penetrated the ultra-secure SWIFT money transfer banking system and stole $81 million from the Bangladesh Central Bank before the New York Federal Reserve Bank discovered the scam and shut it down. The Bangladesh Central Bank used off-the-shelf $10 unsecured routers, enabling the hackers to activate malware inside the bank to infiltrate SWIFT. Although other banks adhere to the highest protocol levels for security, the integrity of the network depends upon the strength of its weakest link, in this case the Bangladesh Central Bank.

Recent infiltrations of healthcare networks through malware worry many provider organizations, yet the resources devoted to cybersecurity lag the needed investment. As organizations merge and enhance their interoperability, the formation of ever larger integrated IT networks presents a problem similar to what compromised the SWIFT network—susceptibility related to the weakest security link in the network.

In addition, the expanded deployment of IoMT devices throughout the healthcare delivery system—at rates many times larger than previously seen—further opens these networks to hacking through IoMT devices with weak security protocols embedded in the medical devices and standalone sensors.

Before IoMT becomes a valuable tool in the delivery of healthcare, IoMT devices require robust security protocols embedded in the devices to protect their connected networks from infiltration by hackers. Provider organizations also must expand their investment in cybersecurity and share best practices throughout the industry.

Failure to put cybersecurity at the forefront on healthcare IT strategy put both patient safety and the protection of personal health information at great risk.



Barry P. Chaiken

Barry Chaiken is the president of DocsNetwork Ltd. and has more than 25 years of experience in medical research, epidemiology, clinical information technology, and patient safety. He is board certified in general preventive medicine and public health and is a fellow, former board member, and chair of HIMSS.

More from this Author

How MACRA will shift providers' IT efforts

EHR vendors raise provider expectations for other IT vendors

New standard can 'FHIR up' precision medicine