HealthManagement.org
Promoting Management and Leadership

Cybersecurity Strategies for Healthcare IoT

The Internet of Things (IoT) enables many of today's devices and equipment to work with such remarkable speed, accuracy and efficiency. Because of the numerous IoT-related benefits, people have a tendency to forget the fact that IoT devices are increasingly vulnerable to hacking attacks.

A new study serves as a timely reminder for hospitals and health systems, where numerous connected devices are commonly found, to ensure IoT security strategies are robust enough to ensure the future of care. The study, by Netherlands-based software firm Irdeto, found that provider organisations lack necessary measures to counter cyberattacks despite being aware of the areas that are vulnerable and need to be protected.

Irdeto researchers, who conducted a survey of 232 healthcare security decision makers, learned that 82% of the surveyed parties had experienced an IoT-focused cyberattack in 2018. One third of the organisations (30%) affected by the attack reported compromised end-user safety.

Interestingly, IT network has been cited by 50% of the respondents as the most prominent vulnerable spot within healthcare organisations. Other areas vulnerable to hacking as noted in the study are 45% of the mobile devices and accompanying apps, followed by 42% IoT devices.

Based on the study findings, network security at healthcare institutions is no longer adequate to prevent significant damage from cybersecurity attacks. Thus, to ensure patient safety, providers need to strengthen their IoT security strategies, according to Irdeto researchers, who point out the importance of implementing security at both the app and device level.

The vast majority of IoT device manufacturers (98%) said that cybersecurity of IoT devices they manufacture or use could be improved either to a great extent or to some extent, the study also found.

In a separate report released recently by ABI Research, financial, information and communication technologies, and defence industries would account for 56% of the £111 billion projected total cybersecurity spend in critical infrastructure for the year 2024. With the remaining 44% of the expenditure divided between the energy, healthcare, public security, transport, water and waste industries, these sectors, without sufficient funding, could be highly vulnerable to cyberattacks according to the report.

Source: ELE Times
Image Credit: iStock

Published on : Tue, 17 Sep 2019