Greatest Cybersecurity Challenge to Connected Device Ecosystem

NEW YORK, Aug. 15, 2017 — More than one-third (35.6 percent) of surveyed professionals in the Internet of Things-connected medical device ecosystem say their organizations have experienced a cybersecurity incident in the past year, according to a recent Deloitte poll. Identifying and mitigating the risks of fielded and legacy connected devices presents the industry's biggest cybersecurity challenge according to respondents (30.1 percent).

"It's not surprising that managing cyber risks of existing IoT medical devices is the top concern facing manufacturers, providers, and regulators," said Russell Jones, Deloitte Risk and Financial Advisory partner, Deloitte & Touche LLP. "Legacy devices can have outdated operating systems and may be on hospital networks without proper security controls. Connected device cybersecurity can start in the early stages of new device development, and should extend throughout the product's entire lifecycle; but even this can lead to a more challenging procurement process. There is no magic bullet solution."

Additional cybersecurity challenges that connected medical devices presented to respondents included embedding vulnerability management into the design phase of medical devices (19.7 percent), monitoring and responding to cybersecurity incidents (19.5 percent), and lack of collaboration on cyber threat management throughout the connected medical device supply chain (17.9 percent).

Jones continued, "Collaboration between providers, manufacturers, and suppliers is key when it comes to bridging the gaps in medical device cybersecurity. This is a problem that requires the industry as a whole to come together and create a safe space where feedback and information can be shared freely."

Beyond cybersecurity risk management itself, there are post-incident risk management efforts to attend to as well. Few respondents (18.6 percent) say their organizations are "very prepared" to address litigation, internal investigations or regulatory matters related to medical device cybersecurity incidents in the next 12 months.

"As regulatory, litigation, and internal investigation activities start to focus on post-market cybersecurity management, leading organizations are taking a more forensic approach to discerning the timeline and size of cyber incidents so the impact to intellectual property, client data and other areas can be addressed more quickly," said Scott Read, Deloitte Risk and Financial Advisory principal, Deloitte Transactions and Business Analytics LLP. "Forensic analyses responding to regulator, litigant, or whistleblower concerns may even help predict the next moves of cyberattackers."

To protect against cyber threats in medical devices, Deloitte recommends a layered approach:

- **Implement a document hierarchy**. Formalize, organize, and structure medical device cybersecurity activities and governance to ensure patient safety and respond more quickly to regulators, legal matters, or internal investigations. Beyond the typical education and training standards and operating procedures, these hierarchies should also include work instructions and templates for each unique device that maps to each component of the product security program. Documentation of quality management system (QMS) protocols and procedures should also be centralized and regularly updated.
- **Conduct annual—at minimum—product security risk assessments**. Treat cybersecurity risk assessment procedures as ongoing, iterative processes that are repeated at least annually and when business changes occur, such as supplier changes, acquisitions, or divestitures. They're utilized throughout the entire lifecycle of connected medical devices—including their related apps—to identify cybersecurity threats that often fall outside of what minimum medical device security requirements address.
- **Take a forensic approach to incident response**. Establish the incident timeline, detect anomalous behavior, and figure out what data was accessed and exposed. Forensic analysis can help your organization uncover facts as well as assist in determining what future actions you need to take in your response and remediation.

About the online poll

More than 370 professionals whose organizations operate in the medical device/IoT ecosystem responded to poll questions during the Deloitte Dbriefs webcast, "Medical devices and the Internet of Things: A three-layer defense against cyber threats," May 23, 2017. Respondent organizations include medical device or component manufacturers (i.e., implantables, diagnostic devices, capital equipment; 31 percent); health care IT organizations (i.e., mobile app/software developers; 22 percent); medical device users (i.e., health care providers, device monitoring; 36 percent); and regulators (10 percent). Answer rates differed by question.