Crowe

Cyberrisk Checkup

Medical Device Risk Management

Issue

Hospitals typically have more medical equipment than IT devices – three to four times more in most cases. And the number of networked medical devices continues to expand. Medical devices that are interconnected can present cybersecurity concerns that put patients' lives at risk. Further complicating the risks, medical devices often are commingled on networks with nonmedical technology such as security cameras, building controls, and telecommunications devices that provide little to no protection from hackers.

Risk Landscape

38%

- HDOs indicating medical devices provided inappropriate treatment/therapy to patients[1]

$5.1 million revenue loss[2]

- Due to patient/customer churn post-breach

$1.1 trillion[3]

- Savings from remote monitoring to improve patient outcomes by 2025

67%

- Medical device makers expecting a cyberattack on one of their devices within the next 12 months[1]

[1] "Medical Device Security: An Industry Under Attack and Unprepared to Defend," Ponemon Institute and Synopsys, May 2017, p. 1. http://www.counciltoreduceknowncybervulnerabilities.org/wp-content/uploads/2017/05/Ponemon-Synopsys-Report-Final.pdf
[2] "2017 Cost of Data Breach Study," Ponemon Institute and IBM Security, June 2017, page 18.
[3] "The Internet of Things: Mapping the Value Beyond the Hype," McKinsey Global Institute, June 2015, page 8.

Action

With little regulation or formal governance, the management and oversight of medical devices poses significant risks to patient safety, care, and operations. This creates legal, financial, regulatory, and reputational threats to healthcare organizations. To mitigate threats and reduce risks, healthcare organizations need to develop an effective cybersecurity risk management strategy that begins with knowing what is on their network. Key elements include:

DISCOVERY

- Locate and track various medical devices and data systems
- Build a comprehensive inventory of medical devices
- Understand third-party support of medical and IoT devices
- Gain visibility into typical usage patterns and behaviors to spot anomalies

RISK FOCUS

- Identify risk factors such as patient safety, unsecure configurations, and value of data
- Prioritize and stratify cybersecurity risks
- Segment or isolate medical devices at greatest risk from other networked devices

STRATEGY

- Establish governance protocols for the addition of new medical devices
- Define roles and responsibilities to identify and manage risks
- Determine which devices to secure and which to isolate
- Reinforce safe technology and systems practices for all networked devices

SUSTAINABILITY

- Implement training programs on alternative procedures in case of device failures, to address patient safety concerns
- Identify and report key metrics
- Implement operating protocols such as changing default configurations
- Regularly perform cybersecurity assessments

For more information on medical device risk management, please contact:

Raj Chaudhary
Principal
+1 312 899 7008
raj.chaudhary@crowe.com

Jared Hamilton
+1 317 706 2724
jared.hamilton@crowe.com

Candice Moschell
+1 (317) 208-2456
candice.moschell@crowe.com

HC-19005-019E