Crowe

Cyber Risk Check-Up

Device Visibility and Network Intelligence

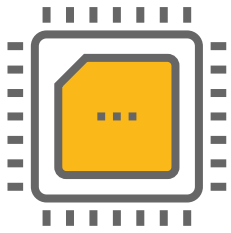
Issue

The fear of medical devices being hacked generates anxiety among both patients and healthcare providers. Often overlooked is the wired and wireless technology intersecting the path of patient care: devices linked into the healthcare system's network, such as internet protocol (IP) security cameras, vendor-monitored control systems for elevators and climate controls, and other technology considered the internet of things (IoT). A breach through any of these devices can shut down a healthcare organization's network and put patients at risk. To have an effective cybersecurity program, healthcare organizations need to begin with a comprehensive inventory of all technology linked into their networks. This includes traditional servers and networks, medical devices used for patient care, and IoT devices.

Risk Landscape

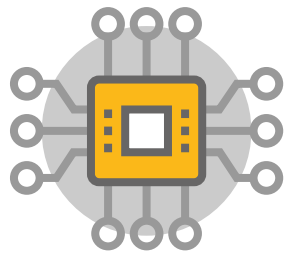
87%

- Healthcare organizations adopting IoT technology by 2019[1]



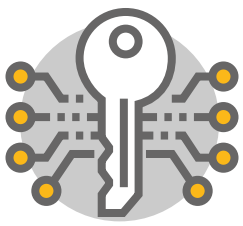
15-17

- Approximate number of medical devices per hospital bed[2]



89%

- Healthcare organizations having already experienced an IoT security breach[1]



47%

- Data breaches identified as malicious or criminal attacks[3]

[1] Heather Landi, "Study: 87 Percent of Healthcare Organizations Will Adopt IoT Technology by 2019," Healthcare Informatics, March 2, 2017, https://www.healthcare-informatics.com/news-item/mobile/study-87-percent-healthcareorganizations-will-adopt-iot-technology-2019

[2] Anthony J. Montagnolo, "Cybersecurity: It's Clinical, Too," ECRI Institute, 2017, https://www.ecri.org/Resources/In_the_News/Cybersecurity_Its_Clinical_Too(Trustee).pdf

[3] "2017 Cost of Data Breach Study: GlobalOverview," Ponemon Institute and IBM Security,June 2017, https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf

Action

A comprehensive device visibility management program is the foundation to addressing the cybersecurity challenges and threats to your healthcare organization, including medical and IoT devices challenges. Crowe healthcare cybersecurity professionals can help you improve cybersecurity posture with device visibility and network intelligence capabilities. Through technology and processes, controls can be enhanced with a structured approach starting with device discovery and understanding of the current state of processes and controls. From there, organizations can begin to develop a strategy for remediation and focus on key risks, with the end goal of building a sustainable program to manage an evolving risk.

Visibility Management Program

	People	Process	Technology	
Discovery	Governance	Control Analysis	Visibility	Quantify Current State
Strategy	Stakeholder Alignment	Complete Visibility	Profiling	Initial Operational Program
Risk Focus	Device Risk Management	Risk Prioritization	Risk Mitigation	Risk-Centered Program
Sustainability	Awareness	Reporting	Tuning	Proactive & Adaptive Management

For more information on device visibility and network intelligence, please contact:

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

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

Chris Reffkin
+1 317 208 2547
chris.reffkin@crowe.com

HC-19005-019C