2017 BURR Alert

Health Care Companies Find Direction to Combat Cybersecurity Threats

By J. Matthew Kroplin and Nicole A. Keefe August 2017

More than 27 million patient records were affected by health care data breaches in 2016, according to a health care cybersecurity company. The cost associated with these breaches is staggering: an estimated $355 per stolen record — the highest among industries surveyed and more than twice the average global cost of a stolen record.

Data breaches can be difficult to detect, which makes this emerging threat an especially dangerous and expensive problem. According to the cybersecurity company's analysis of reported or disclosed health data breaches, it takes more than 200 days for a health care organization to discover a breach — and more than 600 days if the breach came from an insider. Insider incidents, almost evenly divided between human error and wrongdoing, amounted to 43 percent of the reported health data breaches; with hacking and ransomware at 26.8 percent and loss/theft at 19 percent. Cybersecurity threats jeopardize patients, health care providers and organizations, and the industry as a whole.

Proper cybersecurity measures advance both clinical and business objectives in the health care industry by allowing efficient, high-quality patient care while sensibly allocating limited resources. Health care companies are now taking notice of recommendations from the Health Care Industry Cybersecurity Task Force, established by the Department of Health and Human Services as part of the Cybersecurity Act of 2015.

The task force recently outlined recommendations addressing cybersecurity vulnerabilities within the health care industry. The task force, consisting of 21 subject matter experts within and outside of government, concluded that "health care cybersecurity is a key public health concern that needs immediate and aggressive attention."

In the report, the task force identifies six imperatives that must be achieved to increase security within the health care industry, along with recommendations and action items for stakeholders:

1) **Define and streamline leadership, governance and expectations for health care industry cybersecurity.** Recommendations include creating cybersecurity leadership roles; establishing consistent, consensus-based, health care specific guidelines; harmonizing existing and future laws and regulations; and identifying scalable best practices.
2) **Increase the security and resilience of medical devices and health IT.** Recommendations include securing legacy systems; improving manufacturing and development transparency; requiring strong authentication to improve identity and access management; and employing strategic approaches to reduce attack surfaces and interfaces.
3) **Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.** Recommendations include establishing a model for adequately resourcing the cybersecurity workforce; creating managed security service provider

models; and evaluating options to migrate patient records and legacy systems to secure environments.

4) **Increase health care industry readiness through improved cybersecurity awareness and education.** Recommendations include developing executive education programs; establishing a cybersecurity hygiene posture; establishing a conformity assessment model for evaluation; and providing patients with information on how to manage their health care data.

5) **Identify mechanisms to protect research and development efforts and intellectual property from attacks or exposure.** Recommendations include developing guidance for industry and academia on creating economic impact analysis and loss for cybersecurity risk for health care R&D and pursuing research into protecting health care big data sets.

6) **Improve information sharing of industry threats, weaknesses and solutions.** Recommendations include tailoring information sharing for easier consumption; broadening the scope and depth of information sharing; and encouraging annual readiness exercises.

The task force report highlights the benefits of collaboration among stakeholders across the health care industry and encourages cooperation between the public and private sectors to improve cybersecurity. Implementing multiple recommendations will allow organizations to maximize their financial investments and personnel resources to protect the patients served by the health care industry.

To discuss this further, please contact:

J. Matthew Kroplin in Nashville at mkroplin@burr.com or 615-724-3248
or the Burr & Forman attorney with whom you regularly work.

Co-authored with former Burr & Forman summer associate Nicole Keefe, who is currently in her third year at Vanderbilt Law School.