May 2019

South Florida Hospital News™ and HEALTHCARE REPORT

THE REGION'S MONTHLY NEWSPAPER FOR HEALTHCARE PROFESSIONALS & PHYSICIANS

HHS Guide: Steps Toward Cybersecurity

BY JOSEPH RICCIE

Cybersecurity continues to be top of mind these days, especially as we continue to rely on technology and technologies become more sophisticated. On December 28, 2018, a Task Group that includes U.S. Department of Health and Human Services ("HHS") personnel and private-sector health care industry leaders published new guidance for health care organizations on cybersecurity best practices. The guide – Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients – is just that, a guide for healthcare organizations as they begin to navigate the cybersecurity world. This is a start to helping your facility take the steps to becoming cyber secure and helps answer those nagging questions keeping you up at night.

As mentioned in the guide, the Task Force does not expect the practices cited to become a de facto set of requirements that all organizations must implement. Such a dogmatic approach is not effective given the dynamic nature of cybersecurity threats and the fast pace of technology evolution and adoption. Furthermore, they do not guarantee that the suggested practices will aid organizations in meeting their compliance and reporting obligations, but do answer the prevailing questions, "Where do I start and how do I adopt certain cybersecurity practices?"

While it is impossible to address every cybersecurity challenge, the Task Group identifies five prevalent cybersecurity threats.

1. Email phishing attacks – an attacker masquerades as a trusted individual, dupes a victim into opening an email and sending private information – such as wiring money, sending passwords or personal details.
2. Ransomware attacks – malicious software that threatens to publish one's data or block access unless a ransom is paid
3. Loss or theft of equipment or data
4. Insider, accidental or intentional data loss – from employees
5. Attacks against connected medical devices that may affect patient safety

The Task Group also established a set of voluntary best practices and created 10 categories. Each of these categories is detailed within two supplementary technical volumes – one addressing the needs of small organizations and the other addressing the requirements of medium and large organizations – and added resources, including templates and toolkits for determining the cybersecurity practices that would be most effective for your organization.

So what does this all mean? The healthcare industry is one of the most heavily-regulated industries when it comes to cybersecurity practices. Within the Guidance by the HHS Task Force, there are compelling metrics that should lead you to understanding the need for change within your own cybersecurity practices and defenses, and Withum's Cyber and Information Security Team has the experience you need to keep your healthcare organization protected.

Joseph Riccie, Partner, WithumSmith+Brown, PC, can be reached at jriccie@withum.com.