BURR FORMAN LLP

Birmingham Medical News: HHS Publishes Guidelines for Healthcare Providers on Cybersecurity

Articles / Publications
02.27.2019

Reprinted with permission from the *Birmingham Medical News*

On December 28, 2018, the U.S. Department of Health and Human Services and the Healthcare & Public Health Sector Coordinating Councils issued voluntary guidelines to assist healthcare providers to assess cybersecurity risks and suggestions for mitigating those risks. The guidelines, entitled "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" were developed in response to the Cyber Security Act of 2015.

According to the publication, the voluntary guidelines are a collaborative effort of HHS and 150 healthcare and cybersecurity experts. Their approach was threefold: (1) examine current cybersecurity threats, (2) identify specific weaknesses, and (3) provide selective practices to mitigate the threat. The guidance includes a “Main Document” and two “Technical Volumes” with appendices.

What’s Covered – Education and Prevention
The Main Document is intended to educate and raise awareness of cybersecurity issues facing the healthcare industry. It provides definitions and examples. The two Technical Volumes are intended for IT and IT security professionals. Those volumes discuss the ten cybersecurity practices to evaluate for mitigation of risks, broken down by the size of the organization. Lastly, the resources and templates volume contains additional reference materials for healthcare providers dealing with cybersecurity.

RELATED PROFESSIONALS

Angie Cameron Smith

Birmingham Medical News: HHS Publishes Guidelines for Healthcare Providers on Cybersecurity

Because the group determined it was not feasible to address every cybersecurity challenge, it focused on the five most prevalent cybersecurity threats and ten cybersecurity practices it felt were most relevant to the healthcare industry.

The five threats explored in the guidance include:

- email phishing attacks;
- ransomware attacks;
- loss or theft of equipment or data;
- insider accidental or intentional data loss;
- attacks against connected medical devices that may affect patient safety.

For each of the five threats, the guidance defines the threat, provides a real-world scenario, and then suggests the potential impact of each threat. It also gives tips for what to ask, when to ask, and who to ask, if faced with the threat.

The task force also identified potential vulnerabilities tied to each threat. According to the guidance, a threat is anything or anyone with the potential to harm something of value; whereas, vulnerabilities are the weaknesses that, if exposed to a threat, may result in harm and, potentially, some form of loss.

The guidance includes ways to address your organization's vulnerabilities. For example, with e-mail phishing, which is an attempt by a hacker to obtain sensitive or protected information using email, a potential vulnerability is a lack of awareness training. If your practice is the victim of email phishing, you could experience loss of reputation or loss of patients. The guidance then suggests practices consider addressing that vulnerability. This exercise is done for each of the five threats and provides great information that can be used not only to assess your practice but also to educate your staff on cybersecurity issues.

While the Main Document focuses on education, the Technical Volumes deal with prevention using the systems within the organization. There are ten cybersecurity practices or systems healthcare providers should evaluate:

- email protection systems;
- end-point protection systems;
- access management;
- data protection and loss prevention;
- asset management;
- network management;

Birmingham Medical News: HHS Publishes Guidelines for Healthcare Providers on Cybersecurity

- vulnerability management;
- incident response;
- medical device security;
- cybersecurity policies.

The guidance does not rank these practices in terms of importance but states that the provider should determine through an assessment how it would evaluate the ten practices. According to HHS, one of the key aspects of analyzing your cybersecurity needs is determining what size practice you would be under the guidelines. To assist with this analysis, the guidance provides a chart that allows you to determine the best fit for your organization when assessing your cybersecurity needs.

After determining the size of your practice, the provider is then able to choose between volume one for small providers or volume two for medium or large providers. Each volume contains a series of practices for the provider to evaluate within its organization. These are essentially best practices.

Why it's important

One of the most prevalent and costly cyber-threats is Ransomware. According to the HHS, this type of cyberattack has seen a steady increase since its appearance in 2016. Ransomware is malicious software that attempts to deny access to data usually by encrypting the data with a key known only to the hacker until the data's owner pays a ransom. HHS highlighted a Ransomware event that occurred at a rural hospital requiring it to replace an entire electronic health record system.

Some of the statistics provided in the publication included

- Four of five physicians have experienced some form of cybersecurity attack.
  Small businesses constitute 58 percent of malware attack victims costing approximately $2.2 million on average.
  A data breach costs the provider $408 per record.

The guidance provides good information to establish training on the issue and a starting point for policies to help prevent cyberattacks. The Main Document, Technical Volumes, and reference materials can be located at: https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx.

According to the website, Appendix E-1, which is a toolkit to help organizations prioritize their risks and develop an action plan using the methodology contained in the guidance, is still under development, but you can request an advance copy.