Shumaker

MAY 22, 2023 | PUBLICATION

Client Alert: Hospital Cyber Resiliency Initiative Landscape Analysis

Download Client Alert: Hospital Cyber Resiliency Initiative Landscape Analysis

INDUSTRY SECTOR

Health Care

SERVICE LINE

Health Law

RELATED ATTORNEYS

Jarrod J. Malone
Grant P. Dearborn

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

Hospital Cyber Resiliency Initiative Landscape Analysis

Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care

Health and Human Services (HHS) has released a report that details findings about the state of hospital cyber systems across the United States. In connection with a recent Ponemon Institute report on the cost and impact on patient care of cyber-attacks, the reports provide significant and practical insights regarding hospital cyber vulnerabilities and practical effects of such attacks. This data is also of value to other health care entities, such as medical practices and surgical centers.

Summary of Findings:

Ransomware and cyber-attacks are a significant and growing risk in the health care industry. Since 2021, there has been an increase of 50 percent in primary intrusions across industries. Nearly 90 percent of all health care organizations surveyed experienced cyber-attacks in the prior 12 months and the average number of attacks in that period was 43. The average lost productivity as a result of such attacks was $1.1 million.

While 90 percent of hospitals have adopted multi-factor authentication to some degree, this methodology "may not be utilized consistently across key systems and critical entry points."

The report concluded that 89 percent of the surveyed hospitals stated that the facilities conducted vulnerability scans. However, 20 percent or less utilized penetration testing, table top exercises or similar responses. Similarly, a major admitted that the facility did not have a documented plan for addressing any vulnerabilities that were uncovered by the scans. HHS found this to be a significant concern.

A vast majority of hospitals indicated that they have training on cyber related duties and responsibilities. But, the facilities generally lacked data regarding the effectiveness of the training.

Almost 100 percent of hospitals had basic spam and phishing protection capabilities. HHS believed this was

encouraging, but noted that given the current sophistication of attackers, that this may not be sufficient any longer. Of those institutions surveyed, 75 percent also believed their institutions were vulnerable to a cloud compromise.

HHS found that generally hospitals are not sufficiently protected in regard to supply chain vendors use of cyber assets, and the Ponemon survey found 71 percent of respondents say they were vulnerable to supply chain attacks; 50 percent of respondents actually experienced a supply chain attack. Given that a significant number of ransomware attacks originated with third party vendors, HHS believes this is a significant ongoing risk.

While HHS considers medical devices to not typically be exploited to disrupt clinical operations in hospitals, HHS notes that this is still an area that should "warrant significant attention."

HHS opined that the "use of antiquated hardware, systems, and software by hospitals is concerning." HHS is concerned that attackers will exploit known vulnerabilities to compromise older systems. Further, HHS stated that antiquated technologies limit the hospital's ability to protect data.

These reports provide insight into the thinking and expectations of HHS in regard to cyber security and how the practical effect of cyber-attacks are affecting the industry. Moreover, they provide valuable information on the practices of other hospitals, and a view of industry vulnerabilities. Vigilance is always advisable in the cyber world.

Key takeaways include the following:

- Insecure medical devices utilizing mobile apps, such as pacemakers and pumps are at risk.
- Lack of preparedness and collaboration increases risk and ultimate costs.
- Identification of risks must be followed with mitigation efforts.
- Training and awareness programs can significantly reduce risk of phishing and ransomware attacks.