HealthManagement.org
Promoting Management and Leadership

CHIME & AEHIS: Suggestions to Lawmakers for Better Cybersecurity

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) have prepared a written statement for lawmakers offering suggestions for improvement of IT security in healthcare.

Referring to a recent Ponemon Institute report on the dangerous state of healthcare cybersecurity, both healthcare organisations call for more collaboration between medical device manufacturers and providers.

FDA standardisation of a cybersecurity framework for medical devices is also on the list of recommendations in the statement to the Senate Committee on the Judiciary Subcommittee on Crime and Terror.

“While ransomware is the topic of the day, it’s important to take a step back and remember that it is only a subset of the broader cybersecurity threats facing the industry. Additionally, it is important to note that ransomware is just a subset of malware in general, and has been a threat to all industries for over 10 years,” the statement reads.

CHIME and AEHIS also refer to inconsistencies in privacy and security law enforcement.

“The existing enforcement paradigm is heavily focused on compliance with maintaining patient privacy, which can be a distraction or drain on already limited resources necessary to actually secure the numerous points of entry–medical devices, networks, EHRs. Variability in expectations of those that interact with healthcare data, including medical device manufacturers and business associates, will only contribute to the difficultly in securing each and every potential vulnerability,” they say in the recommendations.

They add that to better safeguard healthcare systems, healthcare must improve threat and incident information sharing across the industry. “No single sector of the healthcare ecosystem can solve the problem alone. Only by pulling together and sharing best practices can we thwart cyber criminals and protect patients. This type of collaboration is vital towards remaining nimble to the threats of today, for every day a new threat is introduced into the industry.”

- With this in mind, CHIME and AEHIS suggested lawmakers consider various courses of action to improve cyberhygiene and fight cybercriminals:
- Enabling the Use of a Healthcare-Specific Identification Solution: Reducing the reliance on SSNs and other identifiable information that help bad actors execute fraud will immediately devalue health records on the black market.
- Incentives for Security: Policymakers should look for ways to encourage investment through positive incentives for those who demonstrate a minimum level of cyberattack readiness and mature information

risk management programmes.

- Security as Factor in Reimbursement: Congress should allow CMS to consider a similar principle to value-based reimbursement modifiers to be applied to healthcare enterprises investing in security.
- Reduce Regulatory Complexity: Congress should pursue legislation that harmonises other privacy, security and information risk management requirements to eliminate the complex patchwork of regulations across industries and state lines.
- Workforce Development Programs: Policymakers should support ways to develop security experts to address both cyber concerns and general information security challenges.

Source: CHIME

Healthcare Informatics

Image Credit: Pixabay

Published on : Mon, 23 May 2016