Testimony before the United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Health

Hearing on "Examining Cybersecurity Responsibilities at HHS"

May 25, 2016

Statement of Samantha Burch

Senior Director of Congressional Affairs

Healthcare Information and Management Systems Society

Chairman Pitts, Ranking Member Green and Members of the Subcommittee - Thank you for the opportunity to testify today on behalf of the Healthcare Information & Management Systems Society (HIMSS) regarding our support for H.R. 5068, the HHS Data Protection Act.

HIMSS is a global, cause-based, not-for-profit organization focused on better health through information technology (IT). In North America, HIMSS focuses on health IT thought leadership, education, market research, and media services. Founded in 1961, HIMSS North America encompasses more than 64,000 individuals, of which more than two-thirds work in healthcare provider, governmental, and not-for-profit organizations, plus over 640 corporations and 450 not-for-profit partner organizations, that share this cause.

From our perspective, the organizational change included in this legislation would mark an important step in elevating the critical importance of information and cybersecurity within the Department of Health and Human Services (HHS).

Today's hearing on the HHS Data Protection Act begins a critical conversation that mirrors conversations occurring in healthcare organizations regarding the most effective approach to organizational governance to ensure optimal data flows, processes, and reporting for effective data protection and incident response. Many healthcare organizations now have a Chief Information Security Officer (CISO) and others are in the process of hiring a CISO as the healthcare organization's lead executive responsible for safeguarding data and IT assets.

Cybersecurity has been a growing area of focus for healthcare organizations in recent years. Highly publicized, large-scale breaches of patient and consumer information and other high profile security incidents have impacted both the private and public sectors. Such incidents have included massive amounts of medical information being stolen and sold on the black market at a premium price, hacktivists defacing websites and launching cyber attacks for a political or a socially motivated purpose, hackers leveraging cyber extortion techniques to threaten the release of data in

exchange for the fulfillment of a demand, and ransomware attacks holding medical information and data hostage in exchange for ransom.

Hacking the healthcare sector is now easier and more profitable than ever before. Organized cybercriminals are launching campaigns (such as targeted ransomware campaigns) targeting the healthcare sector. These cybercriminals are more sophisticated and agile than ever before, nearly equaling the sophistication and ability of the highly trained, nation state actor. Non-state actors are also gaining skill and launching effective cyber attacks. Additionally, even those individuals with a relatively low level of skill can successfully conduct cyber attacks (including those types mentioned previously), especially if healthcare organizations have unpatched systems and applications and have vendor default or null passwords—thus, leaving the door wide open to hackers. With so many threats and threat actors—as well as weak cybersecurity—healthcare organizations need a planned, coordinated approach to their cybersecurity programs and initiatives with a CISO at the helm.

HIMSS has spent nearly a decade working to support the healthcare sector's efforts to combat cyber threats. As part of this work, HIMSS released its inaugural 2015 HIMSS Cybersecurity Survey.[1] The concerns of healthcare provider cybersecurity personnel included phishing attacks (69% of respondents), negligent insiders (65%), advanced persistent threat (APT) attacks (63%), cyber-attacks (other than by nation state actors or hacktivists) (59%), and exploitation of known software vulnerabilities (53%). The key takeaways from these findings are that healthcare organizations must focus not only on protecting and defending against external cyber attacks, but also mitigating insider threat such as negligent insider threats (e.g., lost, unencrypted laptops and thumb drives) and malicious insider threats (e.g., breached data due to the actions of a rogue employee or contractor).

[1] http://www.himss.org/2015-cybersecurity-survey

The Evolving Role of the CISO

Elevating the Chief Information Security Officer (CISO) to be a peer of the Chief Information Officer (CIO) reflects the recognition that information security has evolved into a risk-management activity, historically the purview of other executives. In the private sector context, this recognition requires not just a revised job description, but a removal of the traditional subordination of the information security program to the information technology program to create a direct channel to the Chief Executive Officer (CEO), Chief Financial Officer (CFO), General Counsel and other senior executives. Such recognition requires:

- Independence from IT and removal of the inherent subordination of the information security program to the IT program under the current organizational structure,
- A direct channel to CEO, CFO, CCO, GC, etc., and,
- Direct reporting to the Board of Directors (BOD).

Direct reporting to an organization's CEO or other executive management facilitates management of security risk in the context of business risk, which can be operational, legal, and/or reputational. A significant security incident or breach may lead to a disruption in patient care or coordination of patient care. As such, it is clear that healthcare organizations need a cybersecurity leader to manage, as well as mitigate, security risk. Recent surveys find CISOs prefer to report to the CEO, and see the trend moving in that direction.[2,3]

Further, recent studies indicate there are real, positive impacts when the CISO has this reporting structure. "Reporting to the CEO or the Board of Directors, instead of the CIO, *significantly reduces downtime and financial losses resulting from cyber security incidents.*"[4]

As far as operational impact, one study[5] found that "organizations in which the CISO reported to the CIO experienced 14% more downtime due to cyber security incidents than those

[2] http://www.darkreading.com/operations/top-infosec-execs-will-eventually-report-to-ceos-cisos-say/a/d-id/1321980
[3] http://www.klogixsecurity.com/ciso-trends/
[4] http://www.csoonline.com/article/2365827/security-leadership/maybe-it-really-does-matter-who-the-ciso-reports-to.html
[5] http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html

organizations in which the CISO reported to the CEO." And, when the CISO reported to the CIO, financial losses were 46% higher than when the CISO reported to the CEO. In fact, having the CISO report to almost any position in senior management *other* than the CIO (Board of Directors, CFO, etc.) reduced financial losses from cyber incidents.

However, it is important to note that it is not simply the organizational change of the CISO which will dramatically improve the security posture of an organization. The right people, processes, and technology must also be in place. Additionally, information sharing must be encouraged and fostered within the organization. If the CISO does not know about a security incident or other issue, he or she cannot take action to address it.

Positioning HHS to Lead on Security

The August 2015 report[6] on Information Security at HHS prepared by the Committee's Majority Staff raised a number of important points related to the impact of the current HHS CISO reporting structure including lack of prioritization of security concerns and resulting constraints on operating division audits. The report also details the resulting internal security challenges and recent breaches incurred by the Department. This report reflects the seriousness and criticality of the discussion we are having today.

HHS needs security programs in place that support the specific business missions of its various agencies and operating divisions, including: the largest healthcare payer (CMS); the enforcer of HIPAA and holder of associated data on breaches and sensitive private sector company data (OCR); the agency responsible for protecting the public health by assuring the safety, efficacy and security of drugs, biologics, medical devices, products that emit radiation, etc. (FDA); and, the government health research agency (NIH). These agencies represent only a handful of the HHS operating divisions that have experienced data breaches.

[6] https://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/114/Analysis/20150806HHSinformationsecurityreport.pdf

This move would break down silos and put the structure in place to allow the Department to move from an audit-driven approach to security to a proactive and ongoing enterprise business risk management approach to cybersecurity. We also believe that this organizational change would encourage information sharing, but again we emphasize that the organizational culture must also support information sharing about incidents and other potential security issues. Additionally, we believe that external information sharing is essential for HHS with other Federal agencies (such as DHS, FBI, and others) and also with private sector healthcare organizations about the threats which they are facing. Only with a community-based, holistic approach to healthcare cybersecurity can we, as the healthcare sector, collectively improve our security posture and, ultimately, successfully prevent and thwart breaches and other security incidents which may occur.

We see an *important external facing* role for the Office as well. These functions should include:

- Working with the healthcare sector and National Institute for Standards and Technology (NIST) on security best practices and minimum standards for the healthcare industry, consistent with Section 405 of the Cybersecurity Act of 2015, codified at 6 U.S.C. §1533.
- In collaboration with the Office of the Assistant Secretary for Preparedness and Response at HHS, facilitation of cyber threat data sharing between the government and the private sector, and among private sector healthcare entities.
- Development of the security architecture for national initiatives such as the Precision Medicine Initiative and 21st Century Cures.

Advancing Innovation through Trust

Healthcare organizations have come a long way in building the information technology capabilities to make the goals of 21st Century Cures a reality. The HIMSS Analytics Electronic Medical Record Adoption Model (EMRAM) is an 8-step process for tracking progress in building

EMR capabilities.[7] Since the implementation of the HITECH Act, rates of adoption of advanced EMR capabilities have increased significantly. Between Q2 2011 and Q4 2015, hospitals at EMRAM Stage 6 (defined as having structured physician documentation, full clinical decision support and full picture archiving and communications systems) increased from 4.0 percent to 27.1 percent.

The health information contained in these systems holds life-saving potential. These goals are particularly meaningful to me as a five-year survivor of a rare brain tumor and to the HIMSS organization after our colleague and dear friend lost her young adult son to cancer and other complications last week.

We see clearly that it is *trust* that will enable these efforts to succeed - trust in the national program, trust in the system that will house and control access to the patient's data and trust in the public-private collaborative effort. Without this trust that the system will protect data and defend against threats, these efforts simply cannot succeed. Therefore, in order to effectively harness that potential, these ecosystems need a strong security architecture, designed and built-in *from the beginning* of development. The HHS CISO, appropriately positioned within the Department, and empowered with a mandate to focus both internally and externally, will be uniquely qualified to fulfill this important mission.

In closing, I would like to thank Congressman Long and Congresswoman Matsui for their leadership on this legislation and the Subcommittee for prioritizing the issue of cybersecurity at HHS. HIMSS believes the HHS Data Security Act marks a great opportunity to better position HHS to meet the growing challenges of securing health information, information critical to moving the nation's innovation and health agenda forward.

[7] http://www.himssanalytics.org/provider-solutions