HIMSS Cybersecurity Position Statement

Approved by the HNA Board of Directors
September 30, 2016

HIMSS North America

HIMSS Cybersecurity Position Statement

The Health Sector is the Target.

Due to persistent and pervasive cyber-attacks, the health sector's understanding, approach, and sense of urgency around cybersecurity has significantly changed. Previously, the sector focused on privacy and security from the perspective of compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). It was an era in which the biggest threat was an employee losing a laptop or thumb drive with unencrypted data.

Those days are gone.

Today, given the massive amounts of patient information stolen by hackers, cybersecurity is a top concern. Over 85% of respondents to the 2016 HIMSS Cybersecurity Survey[1] reported that information security has increased as a business priority. Further, 77% reported focus on information security due to phishing attacks. If a health organization's security defenses are insufficient, a successful phishing attack may result in a significant security incident that adversely effects the confidentiality, integrity, or availability of information. And, most frightening of all is the potential for patient harm.

The impact of a significant security incident to a healthcare organization is not just financial or reputational. Such an incident may have an adverse effect on patient safety (e.g., a hacked EHR system with tampered information, or a connected medical device under the control of a hacker which may deliver a fatal dose of medicine to a patient). Further, ransomware can cripple patient care by making unavailable essential IT systems and data necessary to provide such care. For all of these reasons, the health sector must holistically approach cybersecurity, and practice defense in-depth.

A proactive approach to security must be the norm, not the exception, to enable trust in, and facilitate collaboration and cooperation amongst, organizations. By becoming more difficult to infiltrate, the health sector will become less of a target by cyber criminals.

[1] The 2016 HIMSS Cybersecurity Survey is available at www.himss.org/hitsecurity.

HIMSS calls on the healthcare community at-large to work together, and with cyber experts from other sectors, to achieve a future state in which all are prepared to defend against increasingly sophisticated and numerous cyber-attacks. We encourage providers, vendors, security researchers, payers, patient-centered groups, policy-makers, and others to proactively exchange information about threats, threat actors, vulnerabilities, and mitigation information.

HIMSS expresses confidence that, through cooperation and focused efforts, we can overcome policy, cultural and financial roadblocks, and other barriers that inhibit the development of cyber solutions that work.

To achieve success, HIMSS recommends the nation take the following actions:

Adopt a Universal Information Privacy and Security Framework for the Health Sector. We must establish a new normal for information privacy and security. We recommend that the health sector adopt a voluntary, universal information privacy and security framework with use cases and implementation guidance—scalable for a wide range of healthcare organizations and inclusive of small, medium, and large providers. The framework must enable use of the tools developed in accordance with Section 405 of the Cybersecurity Act of 2015, specifically the "voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes."[2] While we acknowledge other frameworks could be adapted to fit the health sector's needs, HIMSS recommends NIST's Cybersecurity Framework (NISTCSF).

A universal framework may include: (1) model cybersecurity architectures, (2) model risk assessments, (3) model business associate agreements with security provisions, (4) support for a national strategy around patient and provider identification and matching, and (5) support for individual privacy rights. Existing resources from the public and private sector can be leveraged (e.g., the DHS National Cybersecurity Assessment & Technical Services Program) and new resources can be created, as needed, to support the universal adoption of the framework.

Create an HHS Cyber Leader role. HIMSS recommends the creation of a cyber leader role within the U.S. Department of Health and Human Services (HHS) to be undertaken by an elevated Chief Information Security Officer with internal and external portfolios. We support the White House's announcement to appoint the nation's first federal government Chief Information Security Officer as called for in the Cybersecurity National Action Plan. To advance cyber readiness in the health sector, we need a champion at HHS to encourage stakeholders to be proactive and vigilant about cybersecurity—including the adoption and implementation of a voluntary, universal framework for information privacy and security.

The creation of this cyber leader role at HHS would mark a critically important step in elevating the security posture of health organizations across the nation. With this new role, HHS can lead by example and leverage the capabilities and outreach of Office for Civil Rights, Office of National Coordinator for Health Information Technology, and Office of the Assistant Secretary for Preparedness and Response to help the sector improve its preparedness for and response to security incidents now and into the future.

[2] Section 405 of the Cybersecurity Act of 2015 is codified at 6 U.S.C. §1533 (2016).

In this new role, HIMSS envisions the cyber leader responsible for creating a sector-specific plan to establish goals and priorities for cybersecurity. Examples of these include the following:

(1) ensuring adequate threat and asset response and a plan of action for such effective response, such as through the use of a universal framework for information privacy and security,

(2) encompassing holistic security and what that would entail for the sector (including software manufacturers, medical device manufacturers, healthcare providers, health plans, and others),

(3) fostering interdependence between the health sector and additional critical infrastructure sectors,

(4) expanding the pool of qualified cybersecurity personnel,

(5) advancing workforce education on privacy and security awareness at health-related organizations *and* a plan of action to enable the same, such as through the widespread dissemination of key messages prominently displayed in common areas (e.g., break-rooms),

(6) incorporating lessons learned from Regional Extension Centers and other successful programs to advance greater outreach to small providers,

(7) advancing bidirectional, timely cyber threat information sharing between the Federal government and healthcare sector stakeholders,[3] such as through the National Cybersecurity and Communications Integration Center (NCCIC) and other means,[4] and

(8) advancing the state of health IT and creating a plan of action to ensure that it is created and maintained with privacy and security in mind.

The action steps outlined in the sector-specific plan could be used by stakeholders to create, adopt, and implement robust cybersecurity solutions. HIMSS envisions HHS's cyber leader working with stakeholders to ensure that the plan is a living and breathing document, adapted to the concerns and needs of stakeholders, and kept current. By engaging the whole community to build and deliver cybersecurity capabilities, the sector and the nation

[3] Only 28% of respondents from the 2016 HIMSS Cybersecurity Survey stated that they used an Information Sharing and Analysis Center as a source of cyber threat intelligence. The most common sources were word-of-mouth (62%), healthcare-specific third party vendor feeds (51%), US CERT alerts and bulletins (43%), and FBI-DHS joint indicator bulletins (41%).

[4] An example of a benefit of timely, bidirectional cyber threat information sharing is the exchange of information about a vulnerability on an unpatched system being actively exploited by hackers to manipulate patient information, potentially putting patient lives at risk. The more quickly the vulnerability is fixed by healthcare organizations, the less likely they will be infiltrated by hackers attempting to run such exploits.

will be better prepared to detect, prevent, respond to, and recover from, cybersecurity incidents with less damaging effects.[5]

Address Shortage of Qualified Cybersecurity Professionals. According to the 2016 HIMSS Healthcare Cybersecurity Survey, the top barrier to mitigating security incidents was the lack of appropriately-trained cybersecurity personnel (59% of respondents). The situation could be vastly improved with (1) more educated and qualified cybersecurity personnel (e.g., graduates of the National Security Agency's Centers of Academic Excellence in Cybersecurity) and professionals (e.g., holders of professional certifications like the CISSP, HCISPP, and other credentials), and (2) encouraging innovation with an eye towards more technology-driven solutions for cybersecurity. An HHS cyber leader could convene stakeholders to devise a plan of action to help resolve this shortage at a time when qualified cybersecurity professionals are very much needed.

Conclusion. Cybersecurity is an enabler for the health sector, supporting both its business and clinical objectives and a facilitator of efficient, high quality patient care. Organizations that do not adopt holistic security not only put their data, organizations, and reputation at risk, but also—most importantly—the welfare of their patients. Cybersecurity is no longer optional for any health sector organization.

HIMSS pledges to work with our public and private sector colleagues to ensure all health stakeholders have the tools, resources, information, leadership and expertise needed to protect patients and their data from current and future cyber threats.

[5] Additionally, in the event of a significant cyber incident faced by one or more healthcare sector stakeholders, and consistent with Presidential Policy Directive No. 41, HHS's cyber leader could coordinate with the following agencies: (1) the U.S. Department of Homeland Security for asset response, in the event of a significant cyber incident faced by one or more sector stakeholders, (2) the Federal Bureau of Investigation for threat response, and (3) the Office of the Director of National Intelligence for intelligence support and related activities. Among other benefits, these activities may lead to the successful interdiction of threat actors and the disruption of cybercriminal activity (whether a result of hacktivists, organized cybercrime, nation state actors, or others).