American Hospital Association

800 10th Street, NW
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100 Phone
www.aha.org

Testimony

of the

American Hospital Association

before the

Subcommittee on Intergovernmental Affairs

of the

Committee on Oversight and Government Reform

of the

U.S. House of Representatives

July 18, 2018

Good afternoon, my name is John Riggi and I am the Senior Advisor for Cybersecurity and Risk at the American Hospital Association (AHA). On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, and our 43,000 individual members, I thank you for the opportunity to testify on the important issue of the cybersecurity threats facing hospitals, health systems and the health care field. Today, I will discuss the nature of threats faced by hospitals and health systems, the unique challenges confronting the health care sector, and what the federal government can do to help ensure appropriate protections.

Hospitals, and health care overall, remain heavily targeted by cyber adversaries. The health care field is increasingly realizing the promise of networked information technologies to improve quality and patient safety and bring efficiencies to our systems. But with those opportunities come vulnerabilities to theft and threats to the security of personal information for patients and employees, billing records – even the function of medical devices. Increasingly, bad actors are using phishing emails, malware, and other tactics to attempt to attack hospital computers, networks, and connected devices.

Recently publicized attacks included the use of ransomware – software that holds computers hostage through malicious usage of encryption until a ransom is paid. Other attacks may be motivated by a desire to steal data from a health care system, such as individual medical, financial, or other identity information that can be monetized. In some cases, health care organizations may have intellectual property that is of interest to others. Recognizing that much of the data held by health care organizations is highly sensitive, as well as valuable, hospital and health system leaders are taking cybersecurity challenges extremely seriously and understand that protecting patients and their personal data is a 24/7 responsibility.

UNIQUE CHALLENGES FOR THE HEALTH CARE SECTOR

Health care providers are uniquely and heavily targeted due to the multiple valuable data sets they possess. For instance, recently published data[1] from the Ponemon Institute found the average cost for a lost or stolen health care record was $408 per record. However, the average cost for a lost or stolen record for all industries was much less, coming in at $148 per record. The average cost of a breach for all industries was $3.68 million dollars, while the average cost of a breach for a health care organization was approximately 2.75 times the industry average, or $10.6 million dollars.

Health care is the only economic sector that possesses highly targeted data sets such as personally identifiable information, payment information, protected health information, business intelligence, intellectual property related to medical research and innovation (including genomic studies related to the development of precision medicine), and, as a critical infrastructure sector, national security information related to emergency preparedness and response in times of national crisis or war.

Each one of these data sets are heavily targeted by cyber adversaries. Hospitals and health systems are the only organizations that may possess all of these data sets in combination. Individually, these data sets are highly valuable to the cyber adversary; in combination, they become exponentially valuable.

Also, health care records continue to command a premium price on the dark web because they have enduring value to the cyber adversary. In other words, unlike credit card numbers, one cannot cancel their blood type or a medical diagnosis. Stolen health care records may be the source of repeated health care fraud or be exploited on an ongoing basis for intelligence purposes by a nation-state.

THREATS TO HOSPITALS AND HEALTH SYSTEMS

The main cyber threats faced by hospitals and health care systems are external. They include:

- computer intrusions by external adversaries;
- crypto hijacking;
- business email compromise;
- ransomware attacks;

[1] Cost of Data Breach Study conducted by the Ponemon Institute https://www.ibm.com/security/data-breach

- supply chain attacks;
- data extortion; and
- denial-of-service attacks.

Of these, the most significant and common threats faced by our members include external computer intrusions, which cause the greatest loss of data and bear the highest associated costs in terms of remediation and lost revenue.

A new and emerging threat in 2018 relates to "crypto hijacking" refers to cybercriminals who penetrate a network and take over an organization's high-power computing resources for the purposes of cryptocurrency mining. The unauthorized malware and draining of computer resource may have serious consequences, including the potential disruption of hospital clinical and business operations, along with significant financial costs associated with remediation

Phishing emails continue to be one of the main attack vectors used by cyber adversaries to deliver malware into hospital and health system networks. As a result, hospitals screen incoming email very carefully. It is not uncommon for hospital network defenders to initially block 95 percent or more of incoming email traffic as potentially malicious or spam, accounting for millions of rejected emails every day.

Ransomware also continues to be a major threat for hospitals and health systems. Not only does ransomware hold data captive, it can potentially disrupt clinical and business operations, potentially interfering with the delivery of care and possibly impacting patient safety. More than 200,000 computers in more than 150 countries last year were infected with the WannaCry ransomware worm, which locked down systems and demanded a ransom payment to have them restored. While this attack was waged against all sectors, the health sector drew attention from the media and federal officials because of the critical nature of health care and the widespread impact of the attack on England's National Health Service. The impact on American hospitals and health systems was far less serious, which speaks to the tremendous efforts the field has made to improve cybersecurity and build incident response capabilities.

A WIDE RANGE OF CYBER ADVERSARIES

The U.S. government has attributed last year's WannaCry attack to North Korea. The vast majority of cyber adversaries are based overseas in generally non-cooperative jurisdictions. This general category of cyber adversaries is typically politically or ideologically motivated, such as Hacktivists and terrorists. Thankfully, there have been a very limited number of Hacktivist incidents targeting U.S. hospitals and no known incidences of foreign terrorist organizations conducting attacks against U.S. hospitals and health systems.

Other cyber adversaries include those who are criminally motivated and seek to steal data for illicit financial gain, such as foreign-based cyber organized crime groups. Under this category, health care also faces significant challenges from the criminally motivated insider who steals health records for financial gain and sometimes conspires with an external adversary to enable a cyber attack.

Finally, nation-states posing the most significant threats to hospitals and health systems include China, Russia, Iran, and North Korea. These nation-states, which sometimes operate in cooperation and collusion with criminal organizations, may have unique hacking capabilities. They may target hospitals and health systems to steal data to meet their intelligence requirements, or because of their national security or economic interests. The targeted data may include health records of individuals of intelligence interest, such as government and military personnel, politicians, private individuals possessing security clearances or with access to sensitive information, and individuals of influence.

HIPAA Security Rule Provides Comprehensive Standards for Hospitals and Health Systems

From a regulatory point of view, health care entities already have significant obligations under the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. That rule established a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) has responsibility for enforcing the Security Rule, with civil monetary penalties for violations. OCR has exercised this power in the past and remains a very active regulator. Failure to comply with HIPAA also can result in criminal penalties, and OCR may refer a complaint to the Department of Justice for investigation.

Victims of Cyber Attacks Should be Given Assistance, Not Blame

Despite complying with rules and implementing best practices, hospitals and health care providers will continue to be the targets of sophisticated attacks, some of which will inevitably succeed. The government often repeats the phrase "It's not a matter of if, but when" in regard to an organization becoming a victim of a cyber attack. In fact, as the leader of the Federal Bureau of Investigation's (FBI) cyber national outreach section, I promoted the philosophy that organizations that were victims of breaches should be treated as victims of crime. This approach was subsequently codified in PPD-41.

The victims of attacks should be given support and resources, and attackers should be investigated and prosecuted. Merely because an organization was the victim of a cyber attack does not mean that the organization itself was in any way at fault or unprepared. Similarly, a breach does not necessarily equate to a HIPAA Security Rule compliance failure. In fact, an aggressive regulatory approach could be counter-productive and hinder valued cooperation by the victims of cyber attack with other parts of the government, such as the Department of Homeland Security (DHS), FBI and the intelligence community. Instead, successful attacks should be fully investigated, and the lessons learned should be widely disseminated to prevent the success of similar attacks in the future.

Coordinated Government Support and Partnership are Key to Stopping Cyber Crime

Despite hospitals' concerted attempts to secure their cyber ecosystems, individual efforts to secure systems are insufficient to prevent all attacks. The Administration has used executive orders to name 16 critical infrastructure sectors ─ including health care and public health ─

deemed essential to the security of the nation and directed federal agencies to prioritize securing federal systems. HHS is designated as the liaison for the health care sector. More broadly, the FBI has been designated as the lead authority on investigating cybercrime. Other agencies, including the DHS and the Secret Service, also play key roles in combatting cybercrime and providing guidance. Coordination across these federal resources is critical to ensure threat intelligence and defensive strategies are shared widely, effectively, and in a timely manner. In addition, these agencies must be given the resources to not only respond to attacks, but help vulnerable health care targets prevent attacks from occurring or succeeding on an ongoing basis.

The Cybersecurity Information Sharing Act of 2015 (CISA) provided a mechanism for information sharing among private-sector and federal government entities and provides a safe harbor from certain liabilities related to that information sharing. Information sharing allows organizations to stay ahead of emerging cybersecurity risks and contribute to collective knowledge of threats to guard against. Several private-sector entities, such as the Nation's Healthcare and Public Health Information Sharing and Analysis Center (NH-ISAC) and Health Information Trust Alliance (HITRUST), provide information-sharing opportunities. In addition, the federal government has provided information-sharing resources through its cybersecurity initiatives, including health care and public health facilities. With that said, the goals of information sharing have yet to be fully realized. Expedited and tailored cyber threat information sharing from the federal government would benefit all health care and public health organizations. Providers most need actionable information that identifies specific steps they can take to secure against new threats. Large volumes of more generalized information can prove challenging to interpret, and even become a distraction.

HHS also is directed under CISA to work with the private sector and other federal agencies to establish voluntary, consensus-based best practices. While the federal government is working to provide additional educational and other resources to the health care field overall, more action is needed to address the cybersecurity challenges facing all sectors, including health care. As a nation, we must bolster the security of our cyber ecosystem, not just place the burden on individual institutions. Indeed, the magnitude of the challenges and the growing sophistication of the attacks suggests that the federal government must provide additional nationwide resources. These include efforts to:

- Develop and disseminate coordinated national defensive measures;
- Strengthen and expand our cybersecurity workforce through grant programs and retraining efforts, perhaps with a particular focus on the retraining of veterans;
- Identify and disrupt bad actors;
- Increase the consequences for those who commit cybercrimes; and
- Identify and support best practices by the private sector.

CONCLUSION

Hospitals and health systems are heavily targeted by cyber adversaries, which include sophisticated nation-states. Hospitals and health systems have made great strides to defend their networks, secure patient data, preserve the efficient delivery of health care services and, most

importantly, protect patient safety. However, we cannot do it alone – we need more active support from the government to defend patients from cyber threats. Conversely, the government cannot protect our nation from cyber criminals alone either – they need the expertise and exchange of cyber threat information from the field to effectively combat cyber threats. What is truly needed is the government and health care sector working in close cooperation with a formal exchange of cyber threat information – truly a "Whole of Nation Approach."