States Confront the Cyber Challenge

Cybersecurity in the Health Care Sector

The Threat to the Health Care Industry

The health care industry faces two major cybersecurity threats. First, the transition from paper record-keeping to electronic health records has exposed sensitive personal data previously locked away in cabinets to malicious cyber actors. The industry-wide push to expand the interoperability of these health records has exacerbated the situation by boosting the number of internet access points IT professionals must defend. Because so many health care entities exchange data, it is very difficult for a single company to control and secure customer information. Those in the health care industry who manage technology systems may hold mistaken beliefs about the security of encrypted data.

Another arguably more urgent concern is the vulnerability of hospital equipment and Internet of Things medical devices. Critical lifesaving services may rely on outdated operating systems, outdated hardware and unmonitored connections to vulnerable networks. Adding to those concerns, the rise in telemedicine and mobile application development has led to a growing number of physicians and hospital employees using insecure mobile devices to conduct medical business. However, legacy devices cannot always be updated to fix existing vulnerabilities, while newer equipment may not employ the best security measures. Medical personnel who do not consider cybersecurity on a daily basis may misuse technology, compromising otherwise secure devices. Though IT professionals might recognize the threat and propose solutions, they might lack the necessary support and resources. The industry faces an acute cyber workforce shortage, and existing leadership may not prioritize cybersecurity.

Questions for Governors

- How does my state regulate the health care sector and its various supply chains?
- Which agency can assist health care providers in identifying security vulnerabilities?
- Which state agency will assist health care providers in responding to a cyber incident?
- Which hospitals face the greatest risk of suffering a disabling cyber attack, and what are potential consequences of such an event for my citizens?
- Is my state prepared for a combined cyber-physical attack that uses a cyber intrusion to disable hospital systems following a mass casualty event?
- How can higher education take a more holistic approach to computer science education (for example, integrating coding courses with other academic fields)?

Recommended Steps for Governors

(1) *Convene state health care leaders to elevate cybersecurity as a key issue and generate consensus that cybersecurity is an area for collaboration, not competition.*

Some health care leaders underestimate the potential liability their organizations face. Those who recognize the urgency of the problem may not understand the tremendous value in

working closely with their industry competitors. Governors are in a unique position to introduce these leaders to their counterparts who are moving aggressively to implement stronger cybersecurity practices.

(2) *Gather agency heads and health care CEOs to explore the establishment of a shared security operations center (SOC) to monitor threats*.

An SOC is critical for monitoring, responding to and recovering from cybersecurity breaches. But setting one up is usually resource-intensive and often too costly, especially for smaller health care providers. A public-private SOC could defray those costs and encourage better security practices while giving state agencies instant access to cyber threat intelligence.

(3) *Work with relevant state agencies, including the National Guard and law enforcement, to create a state computer emergency response team (CERT) to assist providers in responding to cybersecurity breaches*.

Many health care institutions cannot afford to hire outside cybersecurity experts to respond to major cyber incidents. Many law enforcement agencies simply cannot respond to a cyber attack. A government CERT, perhaps funded in part by private organizations, would provide a one-stop shop for small and mid-sized businesses in urgent need of cybersecurity advice and technical assistance.

(4) *Encourage widespread adoption of existing frameworks for managing security risks, such as the National Institute of Standards and Technology Cybersecurity Framework or Center for Internet Security Critical Security Controls*.

Collaboration among health care systems will be difficult if those involved do not use similar methods and terminology for managing risk. Advisory bodies already have established cyber risk management frameworks that have been vetted and praised by independent experts. Hospitals and insurers should capitalize on those risk models.

(5) *Promote improved cybersecurity information-sharing through a statewide information sharing and analysis organization (ISAO) and the state fusion center.*

The best cybersecurity practices frequently require widespread information-sharing, but many health care institutions do not receive cyber threat intelligence. The state fusion center is an existing hub for cyber threat intelligence and should consider including health care providers as recipients of relevant cyber threat intelligence. Beyond that, a state ISAO dedicated to cybersecurity would ensure that relevant information reaches all corners of the state's health care sector, sharing signatures of ongoing cyber attacks with potential targets. Fusion centers and ISAOs can anonymize threat intelligence to reassure companies concerned that information sharing could publicize embarrassing news of data breaches prematurely. States should consider coordinating any information sharing proposals with the Health care and Public Health Information Sharing and Analysis Center.

(6) *Consider methods for raising cybersecurity awareness among medical personnel*.

Malicious cyber actors can overcome the best cybersecurity defenses by taking advantage of one mistake by a single employee. Physicians and their support staff must prioritize patient care, but there is room for improving cyber hygiene. With some training and improved procedures, both objectives are mutually compatible. Governors should explore how to debunk common misconceptions and spread a culture of risk awareness among patients and medical personnel.

Please e-mail Timothy Blute, Program Director, Homeland Security and Public Safety Division, NGA at: tblute@nga.org *with any questions.*