AHA Trustee Services

Cybersecurity and Hospitals: A Board Perspective

Cybersecurity is an important issue for both the public and private sector. At a time when so many of our activities depend on information systems and technology, it is not surprising that, when we think about our organizations' vulnerabilities, our information infrastructure must be high on the list. Moreover, hospitals and health systems play a particularly important role because they are part of the United States' critical infrastructure – that is, their systems and assets are considered so vital to the country that their impairment as a result of a cyber attack would pose a threat to the nation's public health and safety.

Members of a hospital's board have the responsibility to understand, at a high level, the risks and vulnerabilities the hospital faces with respect to cybersecurity, as well as the executive leadership's security and response plans.

The Rising Threat

According to data reported to the Office of Civil Rights at the Department of Health and Human Services (HHS), hacking or IT-related incidents in health care compromised the records of 111 million Americans, or one in three in 2015. The largest breaches were health insurers – such as Premera and Anthem. However, we are seeing an uptick in targets on hospitals and other health care providers.

In 2016, we saw the rise of ransomware, and health care organizations were among those frequently targeted. 2017 has brought even more attacks. In May, businesses around the world were affected by the massive WannaCry attack that targeted banking and health care entities in particular, grinding the United Kingdom's National Health Service to a halt. A month later, a form of malware known as Petya infected computers world-wide. Among the hardest hit was Nuance Health Care, a medical transcription software company. Weeks after the attack, Nuance was still struggling to get its systems back online, forcing many hospital and health system customers to implement workarounds.

A successful breach is expensive. Experts estimate the cost to be $363 per record in health care – higher than the $217 average across all sectors in the U.S. – due to the type of information. It is easy to cancel a credit card, but harder to deal with lost medical information.

Who Is Behind the Attacks and Why?

It is important for health care leaders to know who is trying to break into their systems. The goal behind ransomware is almost always financial, and the Federal Bureau of Investigation (FBI) estimates there are over 4,000 ransomware attacks every day. But other bad actors may target intellectual property, such as medical research or financial information held by a health care organization.

The FBI breaks down the bad actors into four groups – each of which can be active in health care.

- Hacktivists generally have a political reason for their actions, or may just want to cause mischief. For example, a children's hospital suffered an attack by hacktivists unhappy with how a particular child's custody was handled.
- Criminals are mostly financially motivated. The recent ransomware attacks fall into this category.
- The advanced persistent threat hacker is often interested in getting large amounts of data. Intellectual property, such as clinical trial data, could be of interest here, as well as large-scale theft of personal, financial, and health information that a hospital may hold.
- Finally, there is always the possibility of a terrorist motivation. This is rare, but health care is critical infrastructure that could be targeted by a nation state or ad hoc group looking to attack. The focus is usually disruption or destruction.

Hospital-specific Risks and Challenges

Hospital risks also may involve patient safety or quality of care. For example, in 2013 the Food and Drug Administration (FDA) highlighted this aspect of cybersecurity when it issued a recommendation that manufacturers and health care facilities ensure that appropriate safeguards are in place to reduce the risk of failure of medical devices due to cyber attack. More recently, the agency issued a recall notice to fix security vulnerabilities in certain pace makers and other cardiac devices. In addition to creating specific damages like those described above, a successful attack would have an impact on the hospital's most important resource – its reputation.

Hospitals and health systems face challenges managing cyber risk:

- Resource constraints
- Challenges recruiting expert personnel, who are in great demand across all sectors
- Dependencies on third-party vendors, including medical device manufacturers, that have not built in adequate security systems

- The sheer complexity of the data systems that they maintain
- Considerable amount of electronic sharing of health information with others who may not have secure systems (submitting claims, sharing clinical data with other providers, reporting to government entities, etc.). This challenge is amplified by federal policies that require information sharing, such as meaningful use.

Finally, law enforcement sees health care organizations that are the victim of a cyber attack as victims. The Office of Civil Rights, on the other hand, sees a cyber attack as a possible breach of protected health information under the Health Insurance Portability and Accountability Act (HIPAA). This can have a chilling effect on organizational willingness to speak up when attacked and share information.

Taking Action

Hospitals are an important component of the Healthcare and Public Health Critical Infrastructure Sector, and take seriously their responsibility to protect their information and other networked systems from unauthorized access and malicious attacks.

In December 2015, the National Institute of Science and Technology (NIST) published its first Cybersecurity Framework for critical infrastructure sectors, which is update periodically. The NIST framework is an important reference for owners and operators of critical infrastructure.

In addition, HHS is currently working on developing cybersecurity guidance for health care providers. While the federal government is stepping up its efforts to provide guidance, challenges remain in making actionable information and resources available to the front lines of health care.

The magnitude of the challenges and the growing sophistication of the attacks suggest that the federal government must provide additional nationwide resources that support all sectors, including health care.

Congress could take steps to fully fund and increase efforts to:

- Identify and apprehend bad actors,
- Increase the consequences for those who commit cybercrimes,
- Develop and disseminate technical defenses,
- Identify and support best practices by the private sector, and
- Build our cybersecurity workforce through grant programs and retraining efforts, perhaps with a particular focus on retraining of veterans.

In addition, the federal government could target solutions specifically for the health care field:

- HHS could provide additional supports and guidance to the health care field, particularly to those with the fewest resources. Supports could include greater availability of guidance, more robust support during active attacks, or opportunities to participate in information-sharing activities that provide specific information on active threats and how to defend against them. HHS also could establish or support a technical assistance center specifically for smaller health care providers. While HHS has made a start in this area, the field could benefit from more, and more specific, supports and guidance.

- The recent ransomware attacks highlighted the extent to which medical devices are vulnerable and create high-risk areas for the security of hospitals' overall information systems. The FDA could provide greater oversight of medical device manufacturers with respect to the security of their products. Manufacturers should be held accountable to proactively minimize risk and continue updating and patching devices as new intelligence and threats emerge. They share responsibility for safeguarding confidentiality of patient data, maintaining data integrity and assuring the continued availability of the device itself. While the FDA has released both pre- and post-market guidance to device manufacturers on how to secure systems, it appears that the device manufacturers have yet to resolve concerns, particularly for the large number of legacy devices still in use. Moreover, while some providers such as the Mayo Clinic have begun to write security requirements into their device procurement processes, more needs to be done to ensure that device manufacturers take their responsibilities seriously.

- Congress could provide specific protections from Stark and anti-kickback penalties for hospitals that want to provide support to community physicians struggling with cybersecurity. Protections already exists for donation of interoperable health information technology and could arguably be extended to also include cybersecurity tools and resources.

AHA Providing Resources and Critical Information

The American Hospital Association (AHA) is continuing to serve as a bridge to federal agencies on cybersecurity issues, working closely with the FBI, Department of Homeland Security and others to share information with hospitals and health systems as quickly as possible in the event of a cyber incident. The WannaCry cyber attack served as a test of our national response capabilities, with HHS Assistant Secretary for Preparedness and Response in the lead for the health sector. The AHA maintained close communications with HHS and shared our resources as they become available from HHS and the FBI. We are also developing an advocacy strategy to create national policies that support the field in meeting the cybersecurity challenge and will continue to provide educational resources to the field.

For more, visit www.aha.org/cybersecurity.

Discussion Questions for Boards

1. Does the hospital have a cybersecurity plan in place that covers all aspects of cybersecurity, not just those associated with personal health information? If so, generally, what is that plan?

2. Who in executive leadership has responsibility for cybersecurity? Is the same person in charge of responding to cyber incidents?

3. When will the board be notified about cybersecurity intrusions or breaches, consistent with your escalation policy? Who will be notified and how?

4. Is there a particular board committee that is responsible for cybersecurity risk oversight? How often is it briefed on cybersecurity matters? How often will the full board be briefed?

5. Does the hospital's current insurance cover cybersecurity incidents? If so, is the coverage sufficient? If not, is cybersecurity insurance warranted?

6. Has hospital leadership considered whether to implement the NIST Cybersecurity Framework or another tool to assess the maturity of your cyber defenses and what the benchmarks would mean for the hospital and its approach to risk management?