Cybersecurity and Hospitals

What Hospital Trustees Need to Know About Managing Cybersecurity Risk and Response

American Hospital Association®

This resources was prepared exclusively for American Hospital Association members by Mary Ellen Callahan of Jenner & Block.

Introduction

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 of directors or board of trustees, although they are not involved in day-to-day management and operations, 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. Some of the risk may be to information. For example, in February 2014, a hospital in Texas notified its patients and former patients that a cyber attack had occurred the previous December, potentially revealing the personal data of more than 400,000 patients. But risks to information also may result in destruction or corruption of patient or billing records, personnel files or disruption of revenue cycle, and even theft of financial and intellectual property.

An article in the July 31 issue of the New England Journal of Medicine (NEJM) urged hospitals to focus on broader cyber threats, such as financial theft, functional interference with medical devices and attacks on critical infrastructure. The article notes that a Washington hospital recently fell victim to a cyber attack perpetuated by Russian and Ukrainian hackers with the help of more than 100 accomplices in the United States. As a result, the hospital lost $1.03 million from its payroll accounts.

The same issue of NEJM also described a sustained cyber attack earlier this year aimed at Boston Children's Hospital's public website. At its peak, the attack significantly slowed legitimate in- and out-bound traffic to the site, essentially making it unavailable for its intended purpose. The attack purportedly was orchestrated by the group Anonymous, a loose and decentralized international network of individuals who engage in hacking for "political" purposes. The group targeted the hospital as a result of a highly publicized custody case in which a child with a complex diagnosis eventually was taken into custody by the state's protective services department. The group threatened retaliation against the hospital if it did not comply with the group's demands, including taking disciplinary action against particular clinicians and returning the child to the parent, even though the child was no longer at the hospital.

Hospital risks also may involve patient safety or quality of care. For example, in June 2013, the Food and Drug Administration 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. 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.

Corporate Governance and Management

Although directors and trustees do not need to know how the hospital handles each cybersecurity risk, the board should be aware of the hospital's plan for managing risk. The threshold questions are:

1. Whether the hospital has a cybersecurity plan in place;
2. Who in management is accountable for developing and implementing the plan, investigating and responding to cybersecurity incidents; and
3. Whether there is appropriate board oversight over the plan.

Cybersecurity Plan. First, what it is not. As part of the hospital's regulatory compliance, it likely has in place a detailed data security plan to protect personal health information (PHI) as required by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).

The board should be aware, however, that cybersecurity is broader than data security associated with PHI. Although data security arrangements may be used to implement aspects of a cybersecurity plan, cybersecurity is not about compliance with regulations and it concerns much more than patient privacy. It is about identifying the systems that are connected to the hospital's information network where the hospital has vulnerabilities – financial data, patient data, personnel files, medical devices – and taking steps to reduce those vulnerabilities. Therefore, it is imperative that the hospital's cybersecurity plan encompass both securing its networks and investigating and responding to intrusions. It also must be broad enough to protect PHI, those systems that store, use or transmit PHI, and all of the hospital's assets and devices. While the board does not need to know all of the details of the hospital's plan, it should at least be aware of the plan's reach and its parameters to ensure that the plan has the ability to address all cybersecurity risks and not just those associated with the potential loss of PHI.

Accountability. The board should know who within the hospital's leadership is responsible for the execution and implementation of the cybersecurity plan. Because cybersecurity is considered one of a number of corporate risks faced by the hospital, it should not be considered solely an information technology issue. Many organizations place responsibility for cybersecurity at the C-Suite level, either as the direct responsibility of the Chief Information Officer or Chief Information Security Officer (CISO), or flowing through the Chief Information Officer's organization up to the Chief Operating Officer, Chief Financial Officer or Chief Executive Officer. Some organizations have placed the CISO within the legal department to incorporate risk management and mitigation holistically.

Oversight. Finally, the board should determine what type of incidents or level of incident will trigger notification of the board. The board likely should not be notified of every cybersecurity incident that occurs. Nevertheless, it may be prudent to have knowledge of the aggregate number of incidents that occur in a given period. The types and frequency of relatively minor incidents are an indication of how the plan is working and whether it is appropriate to the observed threats, so the committee should decide how to be informed of the type and quantity of cybersecurity incidents. Other incidents, however, may be more significant and could have the potential of harming the hospital's operations, finances and reputation. The board likely should know of these more significant incidents and be kept apprised of the investigation, response and, when appropriate, recovery. In general, the hospital's cybersecurity incident response plan should have an escalation policy for major incidents, including when to notify the board of trustees.

Audits and Insurance

Once a board has developed an appreciation for management's assessment of the cybersecurity risks it faces and the resources deployed to reduce these risks, it may wish to consider whether to hire an independent consultant to audit the hospital's cybersecurity program on a periodic basis. This would provide the board with an outside perspective of the cybersecurity risks and vulnerabilities the hospital faces and allow it to work with the executive leadership to resolve them.

In addition, the board should review the hospital's decisions on insurance and, specifically, whether cybersecurity insurance has been acquired and, if not, whether it should be considered. The damages resulting from cybersecurity incidents can be very large, but often these damages are not covered by a hospital's ordinary insurance policies. Some insurance companies now offer plans that specifically cover the risks associated with cybersecurity incidents and breaches. The board should consider, in light of its cybersecurity plan and the hospital's individual risk tolerance, whether cybersecurity insurance of this nature is appropriate.

Other Considerations

Hospitals are considered part of the critical infrastructure of the United States. As a result, the board should keep itself apprised of any relevant developments associated with the president's February 2013 Executive Order on Improving Critical Infrastructure Cybersecurity. Among other things, that order required the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework to provide a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to managing cybersecurity risk; the first version of the Framework was released in February 2014. Although it is not yet mandatory, it is expected that private-sector businesses will be encouraged to voluntarily implement or adopt all or part of the framework. Furthermore, the Cybersecurity Framework may become mandatory for critical infrastructure if cybersecurity legislation passes, or as a *de facto* industry standard. The board should ensure that it is aware of these developments and consult with the hospital's executive leadership on the extent to which the hospital will be adopting all or portions of the framework, and what the hospital benchmarks mean for the robustness of overall cybersecurity protection.

Finally, for hospitals whose stock is publicly traded, the board will need to be aware that in October 2011, the United States Securities and Exchange Commission issued cybersecurity guidance to publicly traded companies. The guidance stated that cybersecurity risks, vulnerabilities and intrusions may trigger a disclosure requirement under a number of areas in a company's 10-K, including Management's Discussion and Analysis, Description of Business, Legal Proceedings and Financial Statement Disclosures. The concept underlying this guidance was that, although cybersecurity and cyber risks are not specifically called out in the current regulations, these issues may be the type that an investor would consider significant to an investment decision and therefore are required to be disclosed. Thus, the board of a publicly traded hospital also should consider these disclosure recommendations as its financial statements are prepared.

Questions for Directors or Trustees to Ask:

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 the 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 the escalation policy?
Who will be notified?

4) Is there a particular board committee that is responsible for cybersecurity?
How often will it be 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 and what the benchmarks would mean for the hospital and its approach to risk management?

Chicago Office:
155 N. Wacker Dr.
Chicago, Illinois 60606
312.422.3000

Washington, D.C. Office:
800 10th Street, NW
Two CityCenter, Suite 400
Washington, DC
20001-4956

www.aha.org/cybersecurity

American Hospital
Association®