BoardBrief

Prepared for Colorado Hospital Association Trustees

Protecting Your Hospital's Confidential Patient Health Information

What Trustees Need to Know About Cybersecurity

Cybersecurity, sometimes referred to as "cyber attacks," cost health care organizations billions of dollars each year. They put patients at risk, resulting in potential patient harm, hospital fines and penalties, and ultimately inflict serious consequences on an organization's community trust and reputation. As stewards of the hospital's financial health and representatives of the community's interests, trustees must take the lead in ensuring that data security and patient privacy are a top priority at their organization.

According to Federal Bureau of Investigation (FBI) Director James B. Comey, the risk of cyber threats is growing, and "has become so dire that cybersecurity has topped the Director of National Intelligence list of global threats for the second consecutive year." In his March 2014 statement, the FBI Director talked specifically about the risk in the health care sector, noting that health care spending consumes approximately 18 percent of the U.S. economy. Because of the prominent role it plays, health care is an attractive target for criminals. But, as Comey noted, it is not a victimless crime. Not only do cyber attacks result in increased costs for health care benefits, insurance, and taxpayers—they also have the potential to "cause actual patient harm, including subjecting patients to unnecessary treatment, providing sub-standard services and supplies, and passing potentially life-threatening diseases due to the lack of proper precautions."[2]

Lost or compromised patient information can lead to financial identity theft, insurance fraud, or to medical identity theft that can plague victims' medical and financial lives for years. It can result in erroneous entries in a person's existing medical records or fictitious medical records in the victim's name. As medical information is shared among hospitals, physicians and insurers, false information can propagate far and wide, leading to a host of problems, including the potential for life-threatening misdiagnoses.

Understanding the Growth of Cyber Threats

The threats associated with cyber attacks have grown significantly in recent years, as nearly all software, devices, and applications now connect to the Internet. Examples include billing systems using electronic transfers, medical devices uploading information real-time into patient electronic health records, and the increase in cloud-based file sharing. The risk grows when organizations consider the use of hospital-issued and personal laptops and mobile devices, and the availability of free Wi-Fi to patients and visitors. The web of data that is available continues to grow, as does the complexity of keeping it secure.

Attacks are Rapidly Increasing. According to the Ponemon Institute's "Third Annual Benchmark Study on Patient Privacy & Data Security," 94 percent of health care organizations have been victims of a cyber attack—94 percent of the surveyed organizations had at least one data breach in the past two years, and 45 percent had more than five incidents during that same time period. This is a drastic increase from 29 percent in 2010.[9]

A separate report released by Redspin in 2014 confirms the trend, reporting that nearly 30 million Americans had their personal health information breached or disclosed since 2009.

7335 East Orchard Road Greenwood Village, CO 80111-2512 720.489.1630 p 702.489.9400 f
www.cha.com

The report identified 199 incidents of breaches of protected health information (PHI) in 2013, impacting over seven million patient records. That's an increase of 138 percent in PHI breaches between 2012 and 2013.[7]

Cyber Threats Vary. One of the more commonly recognized threats are attempts to steal employee and patient data to sell in online black markets. While the reported payment per stolen medical record varies, a recent study reported that the cost to health care organizations is approximately $233 per stolen record, when accounting for incident handling, victim notification, credit monitoring, and projected lost opportunities.[1] Other attacks may be focused on gathering information about medical innovations or technologies, or may be more terrorist in nature, with the goal of harming patients by disabling devices or modifying medical devices.[3]

Eighty-one percent of organizations allow employees and medical staff to use their own mobile devices to connect to their networks. At the same time, only 54 percent report confidence that the mobile devices are secure.[9]

Unsecured Devices and Computers Contribute to Risk. According to the recent Ponemon Institute report, 81 percent of organizations allow employees and medical staff to use their own mobile devices to connect to their networks. At the same time, only 54 percent of the survey respondents reported confidence that the personally owned mobile devices are secure.[9] According to Redspin's President and CEO Daniel W. Berger, portable devices' lack of encryption is one of the greatest risks, stating "It's only going to get worse given the surge in the use of personally-owned mobile devices at work. We understand it can be painful to implement and enforce encryption but it's less painful than a large breach costing millions of dollars."[7]

In addition to unsecured mobile devices, hospitals continually use medical devices that contain sensitive patient information such as radiology imaging software or wireless heart pumps, 69 percent of which are not secure medical devices.[9]

Cloud computing is another risk, with nearly all organizations reporting that they use cloud services. At the same time, 47 percent are not confident that the information on the cloud is secure.[9]

The Financial Impact of Vulnerabilities

Privacy breaches can threaten the short and long term financial health of a hospital. The hospital board has responsibility for compliance, and the Health Information Technology for Economic and Clinical Health (HITECH) Act increased fines for non-compliance with HIPAA privacy regulations to $1.5 million per incident. New privacy and security requirements in the HITECH Act widen the definition of what health care information must be protected and make health care providers and their business associates mutually responsible for protection of shared patient data. The Act also sets specific thresholds, response timelines, and methods for breach victim notification, with potential fines for non-compliance ranging from $25,000 to as much as $1.5 million.

The Economic Impact Continues to Grow. Recent studies estimate that the economic impact of one or more data breaches for a health care organization ranges from less than $10,000 to more than $1 million. However, the average economic impact of a health care organization's data breach in the last two years is $2.4 million.[9]

The Greater Financial Risk May Be Loss of Patient Trust. While fines are significant, damage to the organization's reputation and loss of patient goodwill has the potential for much more devastating and long-term effects than any regulatory penalties. Even more than most business relationships, the provider-patient relationship is based on trust, and when any business loses a customer's personal data, the customer loses trust. A separate Ponemon Institute study found that lost business, not response costs, accounts for 65

Health Care Providers Face Significant Risk

In February 2014, SANS, the largest source for information security training and security certification in the world, published a research study analyzing the impact of cyber attacks on organizations of all types. Data from the health care sector was analyzed from September 2012—October 2013. The report concluded that:[1]

- Health care's critical information assets are poorly protected and are often compromised.
- Providers of all types and sizes are at risk—no health care organization is immune.
- When organizations are compromised, they are often out of compliance for months or longer, meaning they aren't detecting their compromises or outbound malicious communications.
- During the study period, health care providers had the largest percentage of malicious web traffic emanating from them, accounting for 72 percent of all malicious traffic. Health care providers were followed by health care business associates (9.9 percent) and health plans (6.6 percent).

Examples of Recent Breaches

According to a recent report, protected health information (PHI) data breaches increased 138% in 2013.[7] Recent examples include:[6,7,8]

- Theft of four desktop computers from an office at Advocate Medical Group in 2013, which may have exposed more than four million records. Risks associated with unencrypted laptop thefts are growing as more mobile devices are utilized.
- An online security weakness at WellPoint, which serves nearly 36 million people through its affiliated health plans. Unauthorized users accessed personal data for 612,402 people between October 2009 and March 2010, ultimately resulting in a $1.7 million penalty to HHS for HIPAA violations.
- Hacker access to a server containing patient and employee records at St. Joseph Health System in Bryan, Texas in December 2013. While it remains unknown if or how the information will be misused, more than 400,000 people were compromised in the attack.

percent of data breach costs.[5] Based on provider responses and customer loss figures from recent studies, Ponemon estimates that the average health care organization loses over $9 million every two years just to patient churn from data breach incidents, and that privacy-related breaches costs U.S. hospitals almost $6 billion a year. The potential loss may grow further if class-action lawsuits are incurred following a breach.

Board Responsibilities in Cybersecurity

While cybersecurity does not fall into the traditional realm of board roles and responsibilities delegated when hospital boards were first established, today it should be a critical component. Trustees are responsible for protecting both the hospital and its patient community; and data breaches threaten both.

Elevate the Priority. While many health care leaders are aware of the risks, causes of, and ways to prevent data breaches, some continue to believe that prevention of patient data loss or theft is not a priority for their organization.[4] This is where trustee leadership is necessary to bridge the gap between knowing and doing. Security policies and budgets are a governance issue. And to govern effectively, boards need to stay abreast of current trends and methods for improving data security.

According to the recent Ponemon study, the most common causes of data loss or theft were unintentional actions by employees, including lost or stolen computing devices, followed by employee mistakes or unintentional actions. And while the growth in electronic health records (EHR) brings significant potential for improved patient safety and coordination of care, the reality is that electronic records create a new set of security concerns. Digitized records make patient data available to more people inside and outside the hospitals, leaving it vulnerable to hackers and cyber-thieves.

Ensure the Board's Role in Oversight. The American Hospital Association (AHA) recommends that hospital boards assign cybersecurity to a relevant board committee to provide more detailed oversight and governance. The hospital's ongoing cybersecurity investigations and plans should be reviewed with the committee, and, if an intrusion does occur, either the full board or the committee should be briefed on the event, lessons learned, and modifications to the hospital's security plans as a result. The AHA also recommends that the board's audit committee provide oversight into cybersecurity vulnerabilities and potential exposures, including insurance coverage.[3]

Set Security Goals. The board or the appropriately assigned board committee should set privacy and security goals for the hospital. Goal setting should begin with an assessment of current security measure and risks. An expert, objective third-party assessment can measure the hospital's exposure to data breach and whether existing security measures are sufficient. For example, many organizations do not know where all their patient information was physically located or where the greatest vulnerabilities lie. An initial assessment provides a benchmark for setting goals and measuring the success of subsequent security measures.

Staff for Security. Day-to-day security within the hospital environment depends on effective oversight and effective

security processes. Security programs are likely to be more effective if someone in the organization "owns" data security and privacy – usually a chief security officer, chief privacy officer, or compliance officer. If no such position exists, trustees can help assess and determine what kind of staffing will best fit with the organizational structure. Once an owner is in place, the board should support that person with adequate staffing and funding for personnel-related initiatives such as security screening and on-going training in security procedures, in addition to needed system and process improvements.

AHA: Six Actions to Manage Cybersecurity Risks

The American Hospital Association recommends the following six actions to manage hospital cybersecurity risks:[3]

1. Establish procedures and a core cybersecurity team to identify and mitigate risks, including board involvement as appropriate.
2. Develop a cybersecurity investigation and incident response plan that is mindful of the Cybersecurity Framework being drafted by the National Institute of Standards and Technology.
3. Investigate the medical devices used by the hospital in accordance with the June 2013 FDA guidance to ensure that the devices include intrusion detection and prevention assistance and are not currently infected with malware.
4. Review, test, evaluate, and modify, as appropriate, the hospital's incident response plans and data breach plans to ensure that the plans remain as current as possible in the changing cyber threat environment.
5. Consider engaging in regional or national information-sharing organizations to learn more about the cybersecurity risks faced by hospitals.
6. Review the hospital's insurance coverage to determine whether the current coverage is adequate and appropriate given cybersecurity risks.

Sources and Additional Information

1. Filkins, Barbara. Health Care Cyberthreat Report. A SANS Analyst Whitepaper. February 2014.
2. Comey, James B. Director, Federal Bureau of Investigation. Statement Before the House Appropriations Committee, Subcommittee on Commerce, Justice, Science, and Related Agencies. Washington, D.C. March 26, 2014.
3. Cybersecurity and Hospitals. American Hospital Association. 2013.
4. Ponemon Institute. Benchmark Study on Patient Privacy and Data Security. November 2010.
5. Ponemon Institute. 2007 Annual Study: U.S. Cost of Data Breach. November 2007.
6. Landen, Rachel and Conn, Joseph. WellPoint to Pay $1.7 Million HIPAA Penalty. *Modern Healthcare.* July 11, 2013.
7. Sacramento Press Releases: Redspin Reports on the "State of Healthcare IT Security." *PR Newswire.* February 5, 2014.
8. Gregg, Helen. Data Breach at St. Joseph Health System Affects 400K. *Becker's Hospital Review.* February 6, 2014.
9. Ponemon Institute. Third Annual Benchmark Study on Patient Privacy & Data Security. December 2012.