JUNE 2016

trust matters
Trustee Matters
MHA MISSOURI HOSPITAL ASSOCIATION
A Publication for Missouri Hospital Trustees

# Cybersecurity: A Growing Threat for Hospitals and Health Systems

Cybersecurity, sometimes referred to as "cyber attacks," cost health care organizations billions of dollars each year. They put patients at risk, cause hospital fines and penalties, and ultimately inflict serious consequences on an organization's reputation and the community's trust. 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 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 specifically talked 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."

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.

## 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 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.** The average economic impact of a health care organization's data breach in the last two years is $2.4 million.

**The Greater Financial Risk May Be Loss of Patient Trust.** While fines are significant, damage to the organization's reputation and loss of patient

*continued on Page 3 ▶*

# A MESSAGE FROM

## *MHA Board Chair-Elect*
## *Patrick E. Carron, President & CEO*
## *Perry County Health System*

Unfortunately, I can tell you what it feels like to lose sensitive information to a cyber crook. You'll dive head first into the grieving process: denial, anger, bargaining, depression and finally acceptance. Our health system experienced a phishing email scam that compromised our 2015 employee W-2 file. At first, you say, "There's no way!?" Then, your information technology team circles around you with the evidence, your human resources department goes pale, and you feel the adrenalin release.

Now, you're angry. But, that can be motivating. It's the perfect time to channel your anger on the system and not staff. There are so many cyber threats that put every organization at risk. The first question is whether you and your IT team have done everything possible in defense. Staff likely have beaten themselves up over the matter, so there is nothing meaningful a leader can do but to support them through the crisis. Remind yourself that they're probably one step ahead of you in the "process," and that they likely will be there to help you!

In our case, the bargaining phase was mostly useless. There was no one with which to bargain or no price to pay to get the information back. Accept the fact that the best use of your efforts is to begin a defense plan. Having cyber liability insurance is beneficial when a crisis like this occurs. Fortunately, PCHS was able to discuss the problem with an insurance attorney, thus realizing we would make it through alive.

**Tested and True Resolution Plan:**

1. Qualify the scope to determine if public reporting laws apply.
2. Prepare a call center to help staff work through the process of securing their personal information.
3. Develop talking points, news releases, etc., to prepare your public relations department for media inquiries.
4. Formally notify staff of the incident, the organization's investigation, the risks resulting from the incident, and what services and coverage will be made available through the insurance claim.
5. Start working on a better defense going into the future.

When you break the news to the board and staff, they will begin the process with denial and anger. Leadership needs to be patient with staff, media and the larger community. Provide meaningful support by anticipating what actions victims must take to secure their personal information. They will feel more secure after filing a police report, freezing credit reports, notifying the IRS, tightening down financial accounts and increasing security levels on all credit/debit cards, etc. PCHS facilitated many of the steps by supporting victims through the process. PCHS's cyber plan included one year of $1 million in individual protection against financial loss related to risks arising from the claim. Your staff will appreciate the protection.

In closing, you will learn that the work to further protect your organization has just begun. You'll likely begin to tighten down processes and access to sensitive information, both employee and patient. You will develop more detailed policies on who can access sensitive data and how it is transported. You will start testing for weaknesses by modeling cyber criminals, and then rate the system and personnel vulnerabilities. At that point, you will have the information to take specific actions to better defend against outside risks. After a month or two, work life becomes routine again and you can look forward to the next opportunity to take your whole organization through the improvement process that begins again with "denial!"

*continued from Page 1* ▼

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 trust is lost when a customer's personal data is jeopardized. A separate Ponemon Institute study found that lost business, not response costs, accounts for 65 percent of data breach costs. Based on provider responses and customer loss figures from recent studies, Ponemon estimates that the average health care organization loses more than an average of $4.5 million every year from data breach incidents, and that privacy-related breaches cost U.S. hospitals almost $6 billion a year. The potential loss may further grow 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 the prevention of patient data loss or theft is not a priority for their organization. **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 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 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 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 occurs, either the full board or committee should

*continued on Page 4* ▶

## 2016 TRUSTEE RECOGNITION — CONGRATULATIONS!

MHA's Governance Excellence Certificate Program is a voluntary program that provides trustees with the opportunity to learn more about the issues facing their organizations and to develop the skills and knowledge to make more effective decisions. This year, 21 hospital trustees successfully completed MHA's Governance Excellence Certificate Program.

Amy Catron, Cass Regional Medical Center, Harrisonville
Mark Elliff, Mercy Hospital Joplin
Marc Ellinger, Capital Region Medical Center, Jefferson City
Liz Fatka, Western Missouri Medical Center, Warrensburg
Renee Fordyce, Harrison County Community Hospital, Bethany
Amy Freeman, Capital Region Medical Center, Jefferson City
Carla Griffin, Cedar County Memorial Hospital, El Dorado Springs
Greg Hassler, Western Missouri Medical Center, Warrensburg
Lori Herrman, St. Mary's Medical Center, Blue Springs
James Kurzweil, Cass Regional Medical Center, Harrisonville
Mari Macomber, Northeast Regional Medical Center, Kirksville
Debra Ohnoutka, St. Mary's Medical Center, Blue Springs
Larry Purcell, Western Missouri Medical Center, Warrensburg
Sheila Robertson, Harrison County Community Hospital, Bethany
Amy Ryan, Community Hospital – Fairfax
Kirk Sampson, St. Mary's Medical Center, Blue Springs
David Schultz, Putnam County Memorial Hospital, Unionville
Lorelei Schwartz, Capital Region Medical Center, Jefferson City
Nick Wehner, Ste. Genevieve County Memorial Hospital, Ste. Genevieve
Rita White, Western Missouri Medical Center, Warrensburg
Susan Whittle, Barton County Memorial Hospital, Lamar

*continued from Page 3* ▼

be briefed on the event. Lessons learned and modifications to the hospital's security plans should result. AHA also recommends that the board's audit committee provide oversight into cybersecurity vulnerabilities and potential exposures, including insurance coverage.

**Set Security Goals.** The board or appropriately-assigned board committee should set privacy and security goals for the hospital. Goal setting should begin with an assessment of current security measures 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 of their patient information is 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 likely are 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 determine what kind of staffing will best fit with the organizational structure. Once an owner is in place, the board should provide adequate staffing and funding for personnel-related initiatives, such as security screening and ongoing training in security procedures, in addition to needed system and process improvements.

MHA

Trustee Matters *is published quarterly by the Missouri Hospital Association. For questions about hospital governance issues, contact your community hospital.*

*Visit www.mhanet.com for additional health care news.*



**Visit *MHAnet.com/trustees* for additional trustee resources.**