Hospitals In The Crosshairs: Managing Cybersecurity Risk (2)

Anton Janik, Jr.
ajanik@mwlaw.com
(501) 688.8888

08/06/2018

In our last article, we showed you how to evaluate where your organization sits on the landscape of readiness and preparedness. In this concluding article, we identify concrete steps you can immediately employ to move your organization into compliance.

Train Your Employees

Because employees are the leading cause of data breaches, one of the best defenses against breaches is to implement regular employee training as part of your data security plan.

The Federal Trade Commission recommends creating a "culture of security" by implementing and clearly communicating privacy and security policies, regularly training your employees to recognize threats, and identifying clear reporting channels for suspected breaches.[i] Your designated security officer will play a key role in creating and maintaining a culture of security, but the security officer cannot do it alone. The tone is set at the top, so support from board members and hospital administration is critical for success.

Here are some tips for your employee cybersecurity training program:

- Communication. Are your cybersecurity policies communicated regularly in employee orientation, periodic organization-wide training, and in employee policy manuals or handbooks?
- Training. Are you conducting training on a regular basis? Is this training updated as technology, threats, policies or other considerations change?
- Reporting Channels. Are reporting channels clear, simple and easily accessible?
- Active Implementation. Is employee compliance being monitored? Are disciplinary measures imposed for violating security policies? Are employees that identify vulnerabilities publicly acknowledged and praised?
- Testing. Do you regularly test your employees' ability to detect and report on cybersecurity threats like phishing emails?

Keep Your Software Updated

One commonly overlooked protection against cyber threats is updating your software.[ii] Companies that do not update their software on a regular basis may leave open avenues for cybersecurity infiltration and data breach, because programmers regularly identify vulnerabilities in their software and issue patches for them in the form of software updates.

Recent articles discussing North Korea's cyber infiltration teams noted their extensive attacks against computers with unpatched software.[iii] Often, simply installing software updates will eliminate or drastically reduce known vulnerabilities.

Control Data Access

An effective access management plan controls access to data by establishing the "when and how" of appropriate employee access to information and networks,[iv] without hampering legitimate workplace activity. Consider these questions when developing your plan:

- At what points should access rights be required?
- How long should access be permitted?
- When should access be terminated?
- Should access be restricted to just certain files or applications, and what rights should users have to save, print, or transmit data?
- Is there a system for limiting or restricting virtual access to files?
- Which employees should have administrative rights, and to what systems and data?
- Are there limits to third party access?
- Can you encrypt financial and personally identifiable information, whether stored within your system or transmitted elsewhere?

Know Your Vendors and Control Their Activity

The 2013 Target® breach (which resulted in the exposure of credit card and personal data of 110 million consumers) began with an email phishing campaign sent to the employees of a Target® vendor. A key component in mitigating third party risk is to know your vendors and how their activities affect your data security.

Delegating away responsibility for the risk that third-party vendors may lose your customers' data is no longer an option. Prior to selecting a vendor, it is important to clearly identify what legal responsibilities apply to the services in question and how vendors implement the services they provide.[v]

Due diligence should be conducted for any outsourced function,[vi] although the depth of the investigation may vary depending on the scope of the services to be provided. Is an online search for publicly available information or a basic questionnaire about the vendor's cybersecurity precautions sufficient? Or would a more extensive search or vendor questionnaire – or perhaps even an interview or site visit – be more appropriate?

Many of our clients regularly insert cybersecurity warranties and audit requirements in their vendor contracts. Some clients accept vendor self-assessments while others require third party audits, which may include penetration testing, to provide assurances about a vendor's ability to keep data secure. Regardless, due diligence information should be verified and reviewed in the context of your organization's goals and considering the potential impact on your reputation.

Contract review is important to ensure that the client-vendor agreement is consistent with your business needs and complies with your risk management program. Here are some points to consider when negotiating a vendor contract:[vii]

- Limitation of liability. What is the vendor's liability? Are the suggested limits, if any, reasonable given the scope of services and the information that may be impacted?
- Service levels. If a vendor fails to provide the service level standard (e.g., incident response times, data encryption usage) stated in the contract, does that potential failure impact data protection? If so, what is the impact?
- Data protection. Are contractual security requirements specific and measurable for acceptable performance? Are both confidentiality and security covered? Are any types of data excluded from protections? Are there industry standards that can be incorporated to provide acceptable protection?
- Termination. Are expectations set up front about whether a breach of confidentiality or security triggers a termination right?

Mitigating vendor risk doesn't end when the ink dries on the contract. Periodic contract reviews, especially as contract renewals arise, and ongoing monitoring based on the most current legal requirements and industry standards should play an integral part in vendor management.

Create Breach Response Plan

When it comes to breach response, a well-defined plan is vital. At minimum, your plan should identify the response team and set forth any necessary timelines or protocols for carrying out the plan. The response team should include the privacy officer responsible to investigate, analyze, and issue required notifications about the breach, as well as the person responsible for responding to public inquiries.

The plan also should encompass different paths for different types of cyber breaches, for example, a loss of encrypted versus unencrypted data or unauthorized access to financial versus patient-level data. The plan should be regularly reviewed and, if possible, tested with all identified staff taking part.

You also may want to consider whether purchasing cybersecurity insurance makes sense based upon the level of risk your hospital may face in the event of a breach.

Know Your Notification Requirements

If a breach occurs, it is important to know whether you are required to provide notification to those whose data has been compromised. In addition to HIPAA breach notification requirements that may apply, state laws also require notice in some circumstances.

Arkansas has enacted a breach notification statute that requires notice when there is an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business."[viii] If you maintain records for individuals that live in other states, it is important that your data breach response plan also address any applicable notification requirements of those states.

To ensure full compliance with state and federal breach notification requirements, and to determine whether any exemptions are available, seek guidance from your legal counsel for any data breach as soon as possible.

Focus on Flexibility

There is no "one size fits all" cybersecurity risk management program, and once a program is established, the work does not end. Because the technology landscape is constantly changing, regular examination of your cybersecurity risk must be an ongoing component of your hospital's overall operations. It's also important to incorporate cybersecurity into your existing governance, risk management and compliance frameworks. As risks evolve, your staff's continued focus on data security is essential. In the era of electronic health records, ensuring that patient data is safe is a critical component of good patient care.

Republished by permission. This article was originally written for and published in the Summer 2018 issue of Arkansas Hospitals magazine.

---

[i] https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf

[ii] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[iii] https://www.nytimes.com/2017/06/22/technology/ransomware-attack-nsa-cyberweapons.html

[iv] https://iapp.org/news/a/designing-and-implementing-an-effective-privacy-and-security-plan/

[v] https://iapp.org/news/a/third-party-vendor-management-means-managing-your-own-risk/

[vi] https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf

[vii] https://iapp.org/news/a/third-party-vendor-management-means-managing-your-own-risk/

[viii] Ark. Code Ann. § 4-110-102(1)(A).