Overcoming a False Sense of Security in Healthcare

A White Paper

September 2014
Introduction

Recent stats on the prevalence and cost of data breaches in healthcare are staggering:

- There were more than 7 million patient health records breached in 2013, a 138% increase from 2012.¹
- Security breaches, loss of data and unplanned outages cost U.S. hospitals $1.6B each year.²
- In 2013, healthcare-related identity theft accounted for 43% of all identity theft reported in the U.S.³

The number of data breaches reported by health delivery organizations continues to rise, and the consequences of a breach are rising just as quickly. The prevalence of mobile devices in hospitals and physician practices—and the increasing amount of sensitive data exchanged electronically—will only add to the level of risk in the coming year.

This primer looks at how some health delivery organizations currently approach data breaches, and how a false sense of security can be overcome.

A False Sense of Security

The definition of “security” is the state of being free from danger or threat. However, in many healthcare organizations, actual information “security” is not really the goal; compliance with government rules and regulations is the primary focus. Action is taken and money is spent to respond to incidents, but often not to understand and proactively address possible risks.

In fact, limited insight about potential vulnerabilities and perceived compliance with regulatory requirements might actually create a false sense of security. However, no hospital or health system is secure simply because of the following:

1. **No (known) breaches have occurred.** Being free from actual incidents is not the same as being free from threats. A hospital that fails to adequately encrypt end user devices is not secure simply because no one has yet exploited that vulnerability. Amid IT budget and resource constraints, some organizations might feel that “no news is good news” when it comes to data breaches. But the reality is that without any focus on assessing threats, an organization is completely blind to the level of risk—and loss—it is facing.

2. **The organization has received meaningful use incentive payments.** To qualify for meaningful use incentives, health delivery organizations must perform a security risk analysis (SRA) as required by HIPAA. However, the rules do not

---

³ Identity Theft Resource Center via USA Today, February 7, 2014.
specify a certain methodology or framework; and what it takes to be compliant is very different than what is needed to identify and address risks on an enterprise level. Additionally, just because an organization has achieved meaningful use and received an incentive payment does not mean the SRA was performed correctly. According to CMS, inadequate security risk assessments are one of the top reasons that providers fail meaningful use audits. Not only do these organizations have to give back their incentive payments, they are also facing potentially serious and previously unknown gaps in security.

3. A formal security risk analysis has been performed. Even correctly performing a formal SRA does not necessarily mean that an organization is as secure as it could be. There are many tools and methodologies available for conducting an SRA, and not all frameworks are created equal. An information security framework should be comprehensive, be based on regulatory requirements and should include a corrective action plan to track progress. The main goal of an effective SRA is to identify and address any known vulnerabilities.

A Shift in Focus: From “Being Compliant” to “Being Secure”

There are changes to operations, IT management and culture that any organization—regardless of size—can make to better monitor vulnerabilities proactively and address threats before they are exploited.

Operations Changes

- **Establish a security management structure within IT.** For larger organizations, this includes a Chief Security Officer (CSO) or Manager and dedicated support staff. Smaller organizations should at least identify a dedicated IT resource to focus on information security-related responsibilities (performing risk assessments, updating policies, implementing updated procedures and managing the corrective action plan).

- **Coordinate IT Security function with Privacy and Risk Management.** The IT Security function should be closely tied to the existing organizational Privacy and Risk Management functions.

- **Create, update and enforce information security policies.** Security policies for establishing the Security program as well as preventing and responding to security breaches need to be developed, regularly reviewed, communicated to leadership and staff, and then actually enforced.

IT Management Changes

- **Request appropriate budget dollars for security-related items.** Spending can be difficult when budgets and resources are tight, but continuing to invest in information security is absolutely necessary to reduce the risk of exposure. As the IT Department grows, overall investment in security efforts should grow as well.

---

- **Perform annual risk assessments based on a proven, comprehensive framework.** Annual assessments should be thorough and cover all systems. Some organizations might need to start with a smaller scope of systems that process electronic patient health information, but eventually all systems should be assessed for security. A corrective action plan should be developed based on the results of the assessment and a detailed plan put in place to address any risks identified.

**Culture Changes**

- **Change current thinking.** Rather than asking, “What do we need to do to meet regulatory requirements?” focus information security goals on “What should we be doing to anticipate and address all potential threats?”

- **Increase awareness through training.** Minimizing risk of an incident requires awareness from every employee. A little creativity with internal communication and training can go a long way towards raising understanding of risk and preventing a breach.

**The Bottom Line**

Effectively responding to data breaches and complying with HIPAA and meaningful use requirements are important responsibilities that all hospitals and health systems need to take seriously; but that alone does not make an organization **secure.** Proactively monitoring vulnerabilities and addressing threats before they are exploited requires a defined security management structure, regularly scheduled risk analyses, comprehensive assessment and remediation tools based on an industry standard framework and a shift in current thinking.

**About Impact Advisors**

*Impact Advisors provides high-value strategy and implementation services to help healthcare clients drive clinical and operational performance excellence through the use of technology. We partner with industry-leading organizations to identify and implement improvements in quality, safety and value. Our Associates are experienced professionals with deep domain expertise and a commitment to delivering results.*
Impact Advisors has helped many clients address their security needs by drawing upon years of risk assessment experience. Our security methodology provides an efficient and comprehensive approach to conducting a risk assessment as part of a broader Meaningful Use program. Our data collection tools and deliverables were created to efficiently scope, assess and present risk assessment findings and recommendations to client technical experts and senior leadership.

Activities typically performed as part of our security risk assessment methodology include:

- Structured interviews with relevant staff, including: security, compliance, risk management, human resources, data center operations, infrastructure engineers and application analysts
- Comprehensive review of current policies and procedures
- Infrastructure and application testing, as necessary
- Data center review

To learn more about Impact Advisors' approach to conducting a security risk assessment, contact:

Rob Faix: rob.faix@impact-advisors.com or (330) 402-6483
David Flynn: david.flynn@impact-advisors.com or (813) 347-8498

For more information visit: www.impact-advisors.com

Follow us on Facebook and LinkedIn

Copyright © 2014 Impact Advisors, LLC.
All rights reserved.

These materials are provided to you by Impact Advisors as a professional courtesy for personal use only and may not be sold. Please appropriately credit/cite your source as "Impact Advisors, LLC."

All copying for commercial use requires written prior permission secured from impact-advisors.com.