How to Improve Data Security in 2015

by Deborah Juhnke, IGP, CRM

We must first understand where our data is and who has access, an aspect of every good risk analysis of data security.

The Issue

“End-users, sysadmins, and developers lead the pack when it comes to mucking things up, though pretty much all of us are guilty.” These are simple, yet telling, words from Verizon’s 2014 Data Breach Investigations Report.¹ The report statistics indicate:

- Forty-six percent of all data security incidents in health care come from theft or simply losing a laptop or other device containing confidential information—triple that of almost all other industry sectors
- Physical loss is 15 times more common than theft
- Most thefts occur in the work area, followed by homes and vehicles.

The 10th annual Verizon report is compiled from actual data security incidents reported by global law enforcement agencies, information security agencies, forensics organizations, and the Information Sharing and Analysis Center (ISAC), including the National Health ISAC. It finds, “Nine out of ten of all breaches can be described by nine basic patterns.” Almost 75 percent of all health care incidents may be attributed to three of these patterns: physical theft and loss (46 percent), insider misuse (15 percent), and miscellaneous error, such as misdelivery, publication, and disposal (12 percent).

Criminal attacks on health care are increasing, however, rising 100 percent in four years according to the Ponemon Institute’s Fourth Annual Benchmark Study on Patient Privacy & Data Security, now affecting 40% of organizations surveyed. It is important to note that this survey included only covered entities. As we have learned from last year’s Target and Home Depot breaches, the greatest risk for breach may in fact begin with business associates or other third party contractors, as they are often less likely to have sophisticated controls in place.

The health care field shares other characteristics with retail’s visible victims, including a high volume of incidents and slow response times.²

Biggest Worries?

Although employee negligence is considered the biggest security risk by Ponemon (75%), almost the same percentage of respondents (73%) is not confident or only somewhat so that their business associates would be able “to detect, perform an incident risk assessment and notify their organization in the event of a data breach incident…."

And as if these better-known cyber-risks were not enough, there is growing concern that the “Internet of Things”—uniquely identifiable connected devices, such as conferencing systems, medical
devices, web servers, and cameras—is increasingly leveraged to expand the attack surface and carry out denial of service attacks, malware infections, cyber espionage, and data theft.

These vulnerabilities were made visible by the Norse threat intelligence infrastructure during a sample evaluation of the health care sector, collected between September 2012 and October 2013. The analysis showed that 375 U.S.-based health care-related organizations had been compromised (likely unknowingly), ranging from small providers to well-known teaching hospitals. Some examples: 7 percent of malicious traffic came from radiology imaging software, 3 percent from video conferencing systems most likely used for consults and remote procedures, and another 7 percent from video conferencing systems. These types of devices are typically not thought of as being vulnerable to outside attack.

**What Should We Do?**

Understanding that data security threats are a persistent challenge is a good first step. There is no such thing as a one-time project to ensure security, and assuming that the IT department has it covered is shortsighted. There are certainly things that IT must do to harden systems against intrusion, such as changing factory default configurations and passwords, and including other network-attached devices such as surveillance cameras and fax machines in their device list for security controls. (For an example of how simple it is to find and exploit defaults, just do a Google search for “default password.”) True data security, however, relies upon more than just IT controls.

The best way to uncover your own particular vulnerabilities is to conduct a risk assessment. Required by the HIPAA Security Rule for both covered entities and business associates, a well-done risk assessment will help you:

- Identify *all* the storage locations of protected health information (PHI) in your organization;
- Determine the particular threats and vulnerabilities you face—some of which may not be technical at all; and
- Identify compliance gaps and suggest remediation.

Keep in mind that, though necessary and eminently helpful, the risk assessment is not a panacea. We’ve probably all at one time or another taken a test just to get by, only to forget the content or fail to comply with its guidance in the future. A risk assessment, like a driver’s test, is not simply an exercise to get through, but is intended to lead to improvements in performance. Some may also think a risk assessment is simply IT penetration testing—can the “bad guys” get in?—but it is much more than that. Consideration must be given to things as diverse as physical security of both facilities and devices, access authorizations, and termination procedures for employees.

At minimum, HIPAA requires an understanding of where your protected or sensitive data is before you can manage or protect it. That means not only the obvious EHR or billing systems, but also e-mail, mobile devices, laptops, wherever PHI may live.

**But I’m OK if I Out-Source My IT, Right?**

No. In fact, the Ponemon survey found that health care organizations surveyed did not trust their third parties or business associates with sensitive patient info. Ironically, among the top three types of business associates they worry most about are IT service providers. It is understandable that most small organizations must outsource their IT, but be sure not to take the vendor’s compliance for granted.

Due diligence in selecting your business associates, particularly those supplying information technology services, will go a long way toward identifying security weaknesses. Ask about any past incidents, what technology tools they use, and what their encryption practices are. Look at employee turnover, their experience dealing with protected information, and whether they have been subject of an independent audit. These are just a few of the many metrics that support a good due diligence process when selecting vendors. For agreements already in place, there is no time like the present to review them for deficiencies and opportunities for improvement upon renewal. The exercise of simply locating all pertinent agreements may be enlightening!

**Getting Started**

The message for health care providers—from the largest hospitals, to small practices, to continuing care retirement communities—is that the path to improved data security begins with controls to protect us from ourselves. We must first understand where our data is and who has access, an aspect of every good risk analysis of data security. Audit processes, including periodic review of user accounts and logs, can help thwart both
intentional and inadvertent breaches. Protecting the data itself, through encryption and data loss prevention software (DLP), will help minimize the damage when the inevitable happens and someone loses a device.

Above all, however, we must renew our efforts to inform and train our personnel, from the highest executive to the clerical staff. Indeed, the Verizon report notes: “The data seems to suggest that highly repetitive and mundane business processes involving sensitive info are particularly error prone…[and] this pattern contains more incidents caused by business partners than any other.” Training and awareness are both undervalued and underutilized.

- Understand yourself: Perform a risk assessment
- Understand your business associates/contractors: Use good due diligence & contract review practices
- Understand your employees: Provide continual training & security awareness reminders.

References

Need Information about Anthem’s Data Breach?

- www.msma.org/AnthemDataBreach
- www.AnthemFacts.com

As of the time of this printing, Anthem, the health insurance behemoth, announced in early February 2015 that it was the victim of a very large and sophisticated data theft attack. Personal information on some 80 million current and former Anthem customers was breached, including names, addresses, birthdates, and Social Security numbers; all the information necessary for identity theft. At the time of this writing it appears that no medical data or credit card information was stolen, but the scope of the breach is still under investigation.

Anthem says it will inform affected customers by mail before the end of February, and will offer free identity fraud protection. A series of FAQs can be found at www.msma.org/AnthemDataBreach, and Anthem asks all current and former customers to keep a regular eye on a special website it has created to provide updates and guidance. Visit www.AnthemFacts.com

Please feel free to share this information with any of your office staff who currently have or at one time had Anthem coverage.