Reducing security risk using data loss prevention technology

Healthcare organizations should take steps to prevent data breaches, which are on the rise in health care, given that they are somewhat easier to perpetrate than are data breaches in other industries, such as retail or banking, and they tend to be lucrative for the perpetrator.

Information security vendors labeled 2013 the “Year of the Mega Data Breach,” largely on the back of a handful of attention-grabbing data breaches affecting the retail industry. But the healthcare industry has been in the crosshairs of hackers for years. In 2009, the U.S. Department of Health and Human Services (HHS) began posting on its website a listing of data breaches in health care involving the loss of unsecured personal health information, where 500 or more individuals were affected in any given instance: according to this listing, more than 13 million individuals were affected in 2011 alone.

In 2012 and 2013, the number of individuals affected dropped, but the number of entities covered by the Health Insurance Portability and Accountability Act (HIPAA) that reported breaches increased by nearly 30 percent. In 2014, the number of covered entities reporting a breach jumped again by 11.6 percent, and the number of affected individuals doubled, returning to the levels seen in 2011. More than 95 million individuals have been affected already in 2015, largely attributed to the widely publicized breach at Anthem Blue Cross Blue Shield in March.


The exhibit above shows the 277 reported breaches occurring in 2014, broken down by type of breach, based on data provided by HHS. (Note: These data do not include breaches of unknown types and are subject to change with reporting of newly discovered breaches.)

However, a data breach occurs, data loss is a real threat faced by all healthcare organizations—particularly where the data at risk are patients’ personal health information. Moreover, the gravity of this threat in terms of potential financial consequences for patients and the healthcare organization (by way of penalties, fines, and loss of consumer trust) makes it incumbent on finance leaders to play an active role in efforts to safeguard these data. Looking at it another way, the inability to manage the risk and avoid such breaches could have severe financial consequences for the organization.

**Data Worthy of Protection**

Headline-grabbing breaches like those experienced at Anthem Blue Cross Blue Shield leave many asking, “Why health care?” It has been reported that data breaches in health care account for more than 20 percent of all data breaches in all industries worldwide. The exhibit on page 3 shows that healthcare organizations experience far more breaches than other top industries targeted by hackers. Banks and retailers are obvious targets, but the financial value of a health record is not so self-evident. In fact, healthcare information has tremendous value, including after the theft has been detected.

Reuters reports that a single health record can sell for $10 on the black market, or 10 to 20 times the value of a U.S. credit card. The reason for the premium on health records is largely due to the safeguards other industries have put in place. Bank account and credit card data have a very short useful life once a breach has occurred and once the data are used. Banks and card issuers are able to quickly reissue new cards, and fraud-monitoring techniques have advanced to identify

---

suspicious activity. By contrast, a person cannot simply reissue a new set of health data; medical history, prescriptions, diagnoses, and clinical results are unique to each patient. In addition, there is little to no consumer monitoring for misuse of this information, making it ideal for hackers to use to commit insurance fraud or identify theft. For these reasons, it seems likely that attacks on the keepers of this information will continue to gain momentum.

**People, Process, and Technology Safeguards**

To address the increasing likelihood of health records being targeted, the HIPAA Security Rule went into effect in 2005. The rule outlined administrative, physical, and technical controls to protect electronic protected health information (ePHI). These three sets of safeguards were designed to address the people, process, and technology needed for this purpose.

Traditional information security products do an excellent job of addressing the technology aspect of that equation. Antivirus software can combat a virus attacking a laptop or desktop computer. A firewall can help an organization control what is allowed in or out. But the traditional response breaks down in the people and process portion of the safeguards. Covered entities need visibility into what data their users are creating and how they are using the information.

**Introduction to DLP Technology**

Other tools and techniques have been developed to manage the risk posed by threats to data security, and healthcare finance leaders can contribute more meaningfully to efforts to safeguard data within their organizations if they are aware of and understand these tools and techniques.

Data loss/leakage prevention (DLP) technology is a security solution designed to answer three fundamental questions:

> Where are confidential data stored?
> Who is accessing the information?
> How are data being handled?

The answers to these questions provide the basis for a DLP system to detect potential breaches, alert users, and prevent the loss of sensitive information. Users could then generate alerts to be reviewed by stakeholders charged with maintaining data security. DLP technology performs these functions by monitoring sensitive information while in use (endpoint actions), in motion (network traffic), and at rest (disk storage). As effective as this capability sounds, such a system works only if the organization has taken the steps to define what information it considers sensitive and what level of risk it wishes to manage. Organizations define their own level of acceptable risk based on industry regulation and other factors determined by a full risk assessment. Each organization’s interpretation of confidential, sensitive, and public information may differ slightly. Addressing those key points releases the potential for DLP technology to be a powerful behavioral tool that can ensure an organization is operating at the level of risk everyone has agreed to.

DLP technology also can shift the risk ownership back to the departments that are using the data. DLP technology should not be viewed as a tool owned and operated by the IT department. No longer is the CIO or chief information security officer (CISO) the sole person responsible for

---

**TOP 5 SECTORS BREACHED BY NUMBER OF INCIDENTS, 2014**

<table>
<thead>
<tr>
<th>Sector</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health care</td>
<td>120</td>
</tr>
<tr>
<td>Retail</td>
<td>100</td>
</tr>
<tr>
<td>Education</td>
<td>80</td>
</tr>
<tr>
<td>Government and Public</td>
<td>60</td>
</tr>
<tr>
<td>Financial</td>
<td>40</td>
</tr>
</tbody>
</table>

protecting the organization’s sensitive data. Finance has two roles. One is to share responsibility with other departments for protecting the organization’s sensitive data, and the second is to recognize that these risks exist and they either need to be budgeted for (in the case of implementing DLP) or planned for (in the case of preparing for a breach). DLP technology can identify behavior that is violating security policy and empower the CISO to have a conversation with the business unit where such behavior is occurring to determine how best to address it—whether that means authorizing or prohibiting it. Either decision will affect the risk position of the organization.

**Answering the Three Fundamental DLP Questions**

A more detailed look at how DLP answers its three fundamental questions can provide insight into how the technology works.

*Where are confidential data stored?* The first step toward protecting ePHI is knowing where it resides. One of the key tenets of DLP technology is that protecting data security depends on having the ability to discover data at rest. Such data include, for example, ePHI stored in a database, nonpublic information on an internal collaboration tool such as SharePoint, sensitive information in email, spreadsheets on a file server, and notes kept on a desktop or laptop computer. DLP technology has the ability to scour such repositories and identify where the information is stored, making it possible to confirm sensitive information is where it is supposed to be and generate an alert when information is being stored insecurely.

If, for example, the IT team operates a large database for software production, and the development team makes copies of key tables and uses them to test their new release of software—making local copies of certain spreadsheets to be able to work remotely—the DLP technology can use keywords, data pattern matching, and metadata to look deep into files, email, and databases to uncover such sensitive information being stored in places where it is not secure.

*Who is accessing the information?* File-sharing programs, unfortunately, don’t always have the capacity to share information about who created a file, who is using it, or who actually needs access. Although one person may have created the file, the content may be valuable to five other people who need to access it. DLP technology can identify both the creator of the file and who is accessing it. Often, permission to read files in a file share is given to the entire company or to numerous departments simply because the administrator doesn’t know who requires access. Reducing the number of users with access to the repositories where sensitive data are stored could reduce risk exposure. By allowing for creation of a more controlled list of authorized users, DLP technology reduces the risk of unauthorized access.

*How are data being handled?* Information security policies are filled with rules and requirements regarding how users are to interact with information. Always lock your work station. Never write down your password. Encrypt outbound email when

---

**NOVEMBER 2015 healthcare financial management**

---

---
it contains sensitive information. Use only company-approved devices when accessing ePHI.

The problem is that these rules are largely unenforceable, and the more restrictions put in place, the more likely the user is to seek his or her own method for getting work done.

Rather than creating rules and roadblocks, DLP technology can be used to identify risk behavior, so that the offending department can be approached and become a partner in making risk decisions. DLP technology can monitor how the information is being used and trigger alerts when policies are being violated. At that point, the finance, IT, and information security leaders can come together to discuss whether the noted activity should be allowed.

Imagine an office that not only stored health records in an electronic records or imaging system but also printed every record it created. The practice of continuing to print every file and storing them in folders in large file rooms presents a risk. DLP technology would identify the printing activity and provide the event viewer an opportunity to highlight this risky activity. The CISO could then advise the office to consider stopping this activity and, in doing so, reduce the risk exposure.

The financial savings is not the only benefit in such an instance. Because DLP technology is a behavioral tool, it complements many of the organization’s existing security tools and helps leaders focus their security awareness training on topics that have practical application.

When DLP technology detects an email that contains sensitive information, it can either alert the user (reinforcing security awareness topics) or integrate with an existing email encryption solution to automatically protect the sensitive message. When DLP technology detects a sensitive spreadsheet being saved to a USB storage device, it can challenge the user (asking for justification), interact with the endpoint protection software to block access to the USB, or call out to the encryption technology to secure the file before copying it to the storage device.

The effects of data breaches on healthcare organizations can be staggering, and as hackers get smarter, the risk of such breaches will only grow. By answering the three key questions—Where are confidential data stored? Who is accessing the information? How are sensitive data being handled?—hospitals and health systems can mitigate the risk to themselves and their patients.

About the author

John Beeskow, CISSP, is executive vice president of IT, CBI, Detroit (jbeeskow@cbihome.com).

---

Common Causes of Data Breaches in Health Care

In 2014, data loss in the healthcare industry was heavily weighted toward simple theft. Physical property theft—laptops, desktops, printed documents, and other portable storage devices—accounted for 39 percent of reported incidents, affecting 6.9 million individuals.

Unauthorized access/disclosure was the next most common point of compromise, including unauthorized access to email, network server shares, and files stored on desktop computers. An additional 2.9 million individuals were affected by this type of breach.

Hacking or IT incidents made up only 11 percent of the reported breaches, but their impact per breach was the highest (each incident averaged nearly 200,000 records). These attacks included phishing incidents that compromised email accounts, computer virus infections, and server compromises. The potential impact of an unauthorized party accessing the internal systems by these means is exponentially higher due to the larger volume of records in those data stores.