Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

A Framework For Beating Health Care Hackers

Law360, New York (December 17, 2013, 11:24 PM ET) -- Data is going digital, devices are going mobile and technology is revolutionizing how health care is delivered. It seems to be business as usual as your health care organization continues to digitize its operations. You have even taken measures to help guard against the typical risks such as lost laptops, thumb drives and other electronic devices. However, unbeknownst to you, hackers sit in front of their computers looking for ways into your network so that they may surreptitiously peruse through confidential financial records and sensitive patient information.

Unfortunately, this scenario is commonplace and brings with it hefty costs. To the extent electronic protected health information ("e-PHI") is compromised in a cybersecurity breach, health care entities can expect to spend on average $233 per record to clean up the problem. As health care operations digitize, organizations should be cognizant of the cybersecurity risks impacting the data that flows through their systems. Further, health care entities need to understand how to assess and manage these risks to meet Health Insurance Portability and Accountability Act and Health Information Technology for Economic and Clinical Health Act ("HITECH") requirements.

The Facts of Cyber Life

Although health care organizations have not always been a primary target for a cyberattack, hackers are recognizing the value of data held by health care companies. Research indicates that electronic data in the health care sector is among the most vulnerable. Additionally, health care entities account for the highest percentage of incidents, more than one-third of all data breaches in the country. In one report, 94 percent of health care entities have experienced security breaches impacting their data. Moreover, patients have experienced over a 19 percent increase in medical identity theft due to cybersecurity breaches over the last year.

Even given what we know, much of cybersecurity related breaches remains uncertain. There are namely two reasons for this uncertainty:

1. Most cybersecurity breaches go undetected; and
2. Many cybersecurity breaches go unreported.

Across all industries, one report asserted that approximately 69 percent of cybersecurity breaches go undetected. Of those breaches that are detected, 94 percent are unreported until months or longer until finally being discovered.
Why cybersecurity is important now more than ever…

Recently, there has been increased scrutiny given the increased risk of data breaches. The

Health and Human Services, Office of Civil Rights ("OCR") has responded to data breaches by aggressively enforcing HIPAA, which reinforces that compliance with HIPAA requirements is a top priority. Chiefly, the HIPAA breach notification rule was amended to lower the reporting threshold from a "risk of harm" standard to a "probability of compromise" standard. As a result, the health care industry will see increased breach reporting, which will likely result in increased enforcement for noncompliance. This is bad news for health care companies because penalties for noncompliance with HIPAA have also been ramped up under the HIPAA Final Rule promulgated under HITECH.

With an increased focus on data breaches under HIPAA and HITECH, health care organizations don't want to be the last to know how their e-PHI is being compromised. Not understanding the organization's cybersecurity threats can be:

- Bad for patients because it can lead to identity theft;
- Bad for the organization because regulators may use that as evidence of noncompliant security practices; and
- Lead to noncompliance with reporting obligations under HIPAA and HITECH

In addition to increased enforcement on the part of OCR, the Federal Bureau of Investigation has joined the effort to investigate cybersecurity breaches. For example, in October 2013, the FBI opened an investigation of a cybersecurity breach affecting a network of hospitals and clinics, in which someone gained unauthorized access to the medical records of up to 1,800 patients.

The FBI also recognized that collaborative efforts are needed to solve the cybersecurity problem. These include investigating insider threats, detecting external threats and informing the health care industry of cybersecurity threats. However, even with these collaborative efforts, health care organizations must be cognizant that assistance from the FBI could lead to increased scrutiny about the organization's security practices. As such, proactive cybersecurity risk management is the best approach to ensure compliance with HIPAA and HITECH.

What To Do

The stakes are getting higher regarding cybersecurity and HIPAA compliance. However, there are several steps health care organizations can take to protect against cybersecurity data breaches. Further, taking these steps can protect health care companies in the context of increasing investigatory activity on the part of OCR and other agencies, such as the FBI.

First, organizations should conduct periodic risk analyses to determine cybersecurity related risks. The risk analysis can help organizations to:

- Identify key systems and locations;
- Determine where e-PHI is located;
- Identify vulnerabilities and threats;
- Evaluate security safeguards; and
- Evaluate risk to e-PHI.

Second, health care organizations should evaluate whether the draft cybersecurity framework established by the National Institute of Standards and Technology can improve the organization's risk management process. The NIST cybersecurity framework contains

five core elements, which help an organization:

1. Identify critical infrastructure,
2. Protect the organization's critical infrastructure using appropriate safeguards,
3. Detect cybersecurity events,
4. Respond to cybersecurity events using predefined and prioritized activities, and
5. Recover from cybersecurity events to restore critical infrastructure.

The framework's core elements then further subdivide into categories and subcategories and provide cross-references to a number of different standards from industry and government that address each subcategory within those functions. Health care organizations can review these references and select the standard that best addresses the organization's particular needs. Note that the cybersecurity framework is currently open for discussion, which means the components may change when the framework is finalized.

Knowing is Half the Battle

With regard to emerging cyber threats, conducting a risk analysis is key. One of the most critical components of conducting a successful cyber risk analysis includes implementing audit controls with a reporting method to examine system activity. Hackers benefit when their activity goes undetected. Auditing helps to identity and assess system vulnerabilities. Using audit logs and tracking capabilities effectively can help organizations safeguard their systems from intrusion by hackers.

In fact, an audit control framework exists under the HIPAA rules, which require entities to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use e-PHI. Further, OCR has recognized the 16 NIST audit control standards in enforcing the auditing standards. The audit and accountability standards determined by NIST consist of:

1. Developing, documenting, disseminating, reviewing and updating audit and accountability policies and procedures;
2. Coordinating the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
3. Generating audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event and the identity of any individuals or subjects associated with the event;
4. Allocating audit storage capacity onto a different system or media than the system being audited;
5. Responding to audit processing failures;
6. Reviewing and analyzing system audit records for indications of inappropriate or unusual activity;
7. Providing audit reduction and report generation;
8. Using internal systems clocks to generate time stamps for audit records;
9. Protecting information and audit tools from unauthorized access, modification and deletion;
10. Allowing for non-repudiation;
11. Retaining audit records to provide support for the after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements;
12. Providing audit record generation capability for the auditable events;

13. Monitoring information, information sites and frequency for evidence of unauthorized disclosure of information;
14. Providing the capability for authorized users to select a user session to capture/record or view/hear;
15. Providing an alternate audit capability in the event of a failure in the primary audit capability; and
16. Providing methods for coordinating audit information among external organizations when audit information is transmitted across organizational boundaries.

Utilizing these NIST standards can help organizations detect unauthorized activity within systems. Gaining this insight is necessary to identifying effective risk management solutions and strategies.

Managing Cyber Risk is a Top Concern for Various Stakeholders

As data security remains a pain point of organization's operations, corporate executives are getting increasingly involved to manage this risk. As such, the responsibility for protecting against hacking is stretching beyond the duties of organization's IT department as executives increasingly view managing cyber risk to be part of their fiduciary duties. Executives are beginning to appreciate that data breach can seriously impact an organization's bottom line, which has driven them to expand their attention beyond the financial audit process to strategic plans to protect e-PHI and risk mitigation plans for responding to a possible breach. Accordingly, C-level executives and board members are looking for ways to increase their visibility over data security operations through the formation of audit committees and reporting mechanisms.

In addition to the heightened awareness within corporate executive ranks, government agencies are also keenly aware of the need for cooperation across the industry to manage cyber risk. Hackers benefit from lack of awareness and communication across the industry because that allows the hackers to move undetected from one target to the next. Organizations such as the FBI, Internet Crime Complaint Center and the National Health Information Standards Advisory Committee recognize this challenge and are pushing for increased coordination to share information on hacking. Such coordination of information sharing can prove invaluable to health care organizations. The goal of this cooperative effort is to ensure organizations learn about potential data security threats and neutralize those threats before the threats actually impact their systems.

Ultimately, as the health care industry continues to digitize, organizations must be cognizant of the cybersecurity risks affecting their networks, systems and data. Further, as the number of cybersecurity related breaches increases, health care companies must prepare to identify and report such breaches as required by HIPAA and HITECH. Yet, to avoid the pain and cost of recovering from a breach and also paying hefty fines for noncompliance with HIPAA, health care companies should proactively leverage HIPAA risk analyses and the NIST cybersecurity framework to implement effective controls to identify, prioritize, mitigate and monitor risk affecting ePHI.

—By Alaap B. Shah and Marshall E. Jackson, Epstein Becker & Green PC

Alaap Shah is an associate and Marshall Jackson is a law clerk in Jackson Epstein Becker & Green's Washington, D.C., office.