Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Overcoming GRC challenges in the Healthcare Industry

An e-Book publication sponsored by RSA

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives.

RSA

RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats. With RSA's award-winning products, organizations effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud, and cybercrime. In today's competitive landscape, risks are dramatically changing and with increasing complexity, next generation security strategies are critical.

RSA Archer provides GRC professionals with a centralized solution to identify, assess, evaluate, treat, and monitor risks across the lines of business. Areas of focus include IT security and risk management, operational risk, regulatory and corporate compliance, audit management, business resiliency, and third-party governance. For more information, visit www.rsa.com.

Inside this e-Book:

Theranos Oozes With Corp. Governance Lessons

by Jaclyn Jaeger

Ailing biotech startup Theranos just can't seem to stop the bleeding.

Founded in 2003 by CEO Elizabeth Holmes, the healthcare technology company quickly became a Silicon Valley darling—valued at more than $9 billion—for its self-proclaimed "breakthrough advancements" in blood-testing technologies. Theranos claims that it has come up with a way for laboratories to run a broad range of medical tests using micro amounts of blood, rather than the traditional method of drawing several test tubes of blood through a needle in a vein.

Theranos' promising future took a blow last year, however, after a *Wall Street Journal* exposé called its claims into question, alleging that the company is not using its proprietary technology for most of the tests it offers. After the story broke, the Securities and Exchange Commission, the Department of Justice, and federal health regulators launched civil and criminal investigations.

At its core, the question the government wants answered is whether Theranos violated the anti-fraud provisions of federal securities laws by misstating or omitting material facts in connection with the sale of its securities to venture capital firms. "The company continues to work closely with regulators and is cooperating fully with all investigations," Theranos said in a statement.

White

The SEC's investigation of Theranos isn't particularly surprising and may even signal tighter regulatory scrutiny to come for private companies. During remarks made in March at Stanford University's Rock Center for Corporate Governance Silicon Valley Initiative, SEC Chair Mary Jo White revealed that the SEC has a close eye on all "unicorns"—privately held start-ups with valuations exceeding $1 billion. "The concern is whether the prestige associated with reaching a sky-high valuation fast drives companies to try to appear more valuable than they actually are," she said.

"The risk of distortion and inaccuracy is amplified because start-up companies, even quite mature ones, often have far less robust internal controls and governance procedures than most public companies," White added. "Vigilance by private companies about the accuracy of their financial results and other disclosures is, thus, especially critical."

That brings us back to Theranos and the broader corporate governance lessons that its missteps impart on all companies—public and private, large and small. After all, much can be learned about what could happen to a company if its board of directors is not properly structured, or if directors fail to be vigilant, or both.

Suits vs. scientists

Prior to finding itself under the scrutiny of investors and regulators, the composition of Theranos' board did little to improve its image in the public eye. Its former 12-member board of directors at the time was top-heavy with diplomats, military, and political leaders. Aside from Holmes herself, other members included former Secretaries of State Henry Kissinger and George Shultz, former senators Sam Nunn and Bill Frist, a retired Marine Corp general and a retired Navy admiral.

Last year, however, amid the scrutiny, Theranos decided to downsize its board to five members and renamed it a "governing board." It also established a newly formed "board of counselors" to act as an adviser to the company, and further established a separate scientific and medical advisory board.

On May 12, 2016, Theranos announced that Sunny Balwani, its president and chief operating officer, will be leaving the company. It also added three new board members as part of its restructuring.

The newly added members include Fabrizio Bonanni, who retired in 2013 from his role as executive vice president at biotechnology company Amgen. "Bonanni will work in a special capacity with management as it builds on its operations and quality systems infrastructure," Theranos said.

> "The risk of distortion and inaccuracy is amplified because start-up companies, even quite mature ones, often have far less robust internal controls and governance procedures than most public companies."
>
> Mary Jo White, Chair, Securites and Exchange Commission

The other two additions to the board, both of whom formerly served on Theranos' board of counselors, will now have "a more direct role in decision-making and shaping the company," Theranos said. These members are William Foege, former director of the Centers for Disease Control and Prevention, and Richard Kovacevich, former chief executive officer of Wells Fargo.

Furthermore, Theranos said it expanded its scientific and medical advisory board by adding several new laboratory and medical experts in the relative fields of pathology, immunology, and epidemiology. "The board was expanded after the company hosted three scientific review sessions with leading laboratory and medical experts who were invited to review the company's proprietary technologies. Theranos provided the experts full exposure to its systems, devices, and data," the company stated.

It appears to be trying to clean up its tainted image. "The independent experts reviewed development and validation reports for tests performed on small-volume samples, including finger-sticks, using Theranos' proprietary technologies for a variety of assays, including assays of their choice," the company added.

Responsibilities of the scientific and medical advisory board include working alongside Theranos' leadership and internal teams in various areas, "including advising Theranos regarding the full integration of its technology into routine clinical practice, and publication and presentation in scientific journals and at scientific meetings," the company stated. "The members who are laboratory directors in their own institutions will work with the company to help inspect its clinical laboratories, and help the clinical laboratory directors with the implementation of best-in-class lab procedures and processes."

A board of advisers plays a different role than a board of directors, and it may be wise that a company consider having both at the outset, which Theranos did not. "An advisory board doesn't have the fiduciary obligations that a board of directors does," explains Peter Gleason, president of the National Association of Corporate Directors. "They're usually paid advisers in a specific technical area." Directors, on the other hand, have fiduciary duties that they are obligated to fulfil to shareholders of the company, and they have legal obligations with liability attached to their role.

Theranos did not reply to requests for comment.

Board dilemmas

The issue faced by Theranos is one that all companies face: How to balance having enough industry expertise on the board to keep it relevant, but not so much as to tip it away from the strategic operations of the company.

"Venture capital companies very often will have people that are representative of stakeholders or investors, as opposed to independent directors brought in because of their expertise or connections in various core competencies," says Richard Morris, a partner with law firm Herrick, Feinstein.

The benefit of having a subject-matter expert is that "they have more knowledge, so they can ask better questions," says Morris. At the same time, you have to be careful not to load the board with too many subject-matter experts, because they're not there to provide advisory services to the board. "They are there as a director," he says.

Any time a company brings a subject-matter expert onto a board, however, it must be mindful of conflicts of interest, corporate governance experts warn. An organization could run into non-compete issues, for example, if it appoints a director to its board who has recently retired from a competitor.

Directors must work together "to have meaningful conversations and to address and complement each other's core competencies," agrees Morris. What the board is trying to do is obtain the information it needs to help the company develop strategy and assess the risks of the enterprise in a professional and prudent manner.

Independence, like integrity, is critical and underpins everything. Theranos might learn this lesson the hard way, given that David Boies, who sits on the governing board, also acts as the company's outside legal adviser.

Depending on how the government investigations unfold, Boies may find himself in a position where he has to either represent the company as its legal adviser or its shareholders in his capacity as a director.

The culture of the board plays a valuable role; the types of behaviors directors need to demonstrate to achieve this are open-mindedness and the ability to foster constructive dialogue. This means being able to challenge management, while still contributing to a productive and collegial boardroom environment, which requires mutual respect.

GETTING TO KNOW THE BOARD

Below are excerpts from Theranos' medical and advisory board's biographies.

Susan Evans, PhD. Evans has over 30 years of experience in diagnostics and health technology companies. She served as president, secretary, and member of the board of directors for the American Association for Clinical Chemistry (AACC). She also served as president of the National Academy of Clinical Biochemistry

William Foege, MD. Foege is an epidemiologist and former director of the U.S. Center for Disease Control and Prevention, He is recognized as the health innovator behind the successful campaign to eradicate smallpox in the 1970s. Foege was a senior medical adviser for the Bill and Melinda Gates Foundation from 1999 until his retirement in 2011.

Ann Gronowski, PhD. Gronowski is a professor in the Department of Pathology and Immunology and the Department of Obstetrics and Gynecology at the Washington University School of Medicine in St. Louis. She is board certified in Clinical Chemistry and is co-medical director of the clinical chemistry, serology, and immunology laboratories at Barnes-Jewish Hospital.

David Helfet, MD. Helfet is the director of the Orthopedic Trauma Service, Hospital for Special Surgery and New York-Presbyterian Hospital, and Professor of Orthopedic Surgery, Weill Cornell Medicine. He is former president of the Orthopaedic Trauma Association.

Larry Kricka, D. Phil. Kricka is a professor of Pathology and Laboratory Medicine at the University of Pennsylvania and was director of the General Chemistry Laboratory and the Endocrinology Laboratory at the Hospital of the University of Pennsylvania. He is a Fellow of the Royal College of Pathologists, and a member of the Editorial Board of Clinical Chemistry.

Jack Ladenson, PhD. Ladenson is the Oree M. Carroll and Lillian B. Ladenson Professor of Clinical Chemistry at Washington University School of Medicine. He has been active in a number of professional organizations and has served as president of the AACC and the Academy of Clinical Laboratory Physicians and Scientists.

Andy Miller, MD. Miller is an assistant attending physician in Infectious Diseases at the Hospital for Special Surgery and New York -Presbyterian Hospital, and an assistant professor of clinical medicine at Weill Cornell Medicine. His areas of clinical expertise and research activity are orthopedic and rheumatologic infectious disease.

Steven Spitalnik, MD. Spitalnik is a professor of Pathology and Cell Biology and vice chairman of laboratory medicine at Columbia University Medical Center. As the medical director of the clinical laboratories on the CUMC campus of the New York-Presbyterian Hospital, he coordinates the clinical service, educational, and scholarly activities of the Division. In addition, he is the co-director of the Laboratory of Transfusion Biology.

Source: Theranos.

An ineffective board, thus, is one with a dominant CEO who is not letting any of that dialogue happen and is pushing forward with the agenda no matter what, says Gleason. The board effectively isn't afforded the time it needs to have constructive dialogue around critical issues that need to be addressed and, instead, simply hear presentations from management rather than engaging with management, he says.

The size of the board, which generally correlates to company size, is also an important consideration. "There is no magic number, but you want to have a number that is conducive to good dialogue, so you're not over-relying on one person versus another person, that you're getting feedback from a variety of perspectives and a variety of individuals," says Gleason.

Director tenure and age are also important factors. Before Theranos restructured its board, the average age of directors was 80, which raised questions about their real level of familiarity and knowledge of emerging economic and technological trends in the fast-evolving science and medical fields.

According to newly revised Global Governance Principles issued in March by CalPERS' Investment Committee, boards should consider "all relevant facts and circumstances" to determine a director's independence, including the director's years of service on the board. "We believe director independence can be compromised at 12 years of service. In these situations a company should carry out rigorous evaluations to either classify the director as non-independent or provide detailed annual explanation why the director can continue to be classified as independent," CalPERS stated.

Additionally, CalPERS recommended that boards have routine discussions "as part of a rigorous evaluation and succession planning process surrounding director refreshment to ensure boards maintain the necessary mix of skills, diversity, and experience to meet strategic objectives."

Imagine, for the sake of argument, that Theranos was found in violation of the anti-fraud provisions of federal securities laws. That does not necessarily mean the directors themselves breached their duty of care. "Directors are not guarantors," says Morris.

In the event of an investigation and alleged wrongdoing, directors are allowed to rely, to a reasonable extent, on the due diligence of legal, audit, and other experts. Theranos' board, for example, likely would have relied on the company's officers to attest to the validity and accuracy of the reports it received about the company's lab conditions and procedures.

To be found not liable, however, the directors would have had to properly exercised their fiduciary duties of good faith, care and loyalty, which would include being reasonably prudent, says Morris. That would require taking a close look to determine the sufficiency and effectiveness of the policies and procedures of the company, based on the information they receive from company officers and other experts, as well as their own expertise, he says.

"It's really hard to detect fraud from a board of directors' standpoint," says Gleason. If someone is intentionally trying to commit fraud from within management, and that management team is providing the board with information they were reviewing, detecting the problem can be very difficult.

Affording directors time to have open dialogue and being able to provide their insight, is critical. "If I just show up at a meeting and listen to 15 presentations and leave, what did you really get from me? What's my value add?" says Gleason.

"Boards should be engaged," Gleason adds. "They bring their experience. They bring their insight. They bring their expertise to the table to help the company move forward. If you don't take advantage of that, you're missing that opportunity." ■

THERANOS RESTRUCTURING

Theranos in May made further changes to the board of directors, as the ailing biotech start-up faces civil and criminal investigation into whether it defrauded investors. The company also announced the retirement of Sunny Balwani as president and chief operating officer.

The latest additions to Theranos' board include Fabrizio Bonanni, retired in 2013 from his position as executive vice president at independent biotechnology company Amgen. In his 14 years with Amgen, Bonanni, served in numerous roles, including as senior vice president, quality and compliance and corporate compliance officer; senior vice president, manufacturing; and executive vice president, operations, overseeing the company's global production and supply chain activities, as well as quality, process development, drug delivery devices, engineering, and environment, health, and safety.

While the company expands its executive team, Bonanni "will work in a special capacity with management as it builds on its operations and quality systems infrastructure," Theranos said.

The other additions to the board will have a "direct role in decision-making and shaping the company," Theranos said. These members include William Foege, epidemiologist and former director of the U.S. Centers for Disease Control and Prevention, and Richard Kovacevich, former chief executive officer of Wells Fargo.

Foege has been working closely with the company and the scientific and medical advisory board as Theranos prepares to publicly introduce its technologies. Both Foege and Kovacevich previously served on Theranos' board of directors before joining its board of counselors, an advisory group. Foege also serves on the company's scientific and medical advisory board.

Theranos said it's also implementing a new organizational structure with dedicated corporate divisions for technology and clinical operations. The company has been undertaking searches for multiple executive positions, and Balwani "will continue to support the transition process through its completion," Theranos said.

The appointment of Bonanni and the other board members comes a month after Theranos expanded its scientific and medical advisory board, whose members advise the company on the integration of its technologies into routine clinical practice, the upcoming publication and presentation of its work in scientific journals and at scientific meetings, and other clinical initiatives.

—Jaclyn Jaeger

RSA®

Harness Risk, Fuel the Enterprise RSA Archer

Preparing for a HIPAA Compliance Audit

by Jaclyn Jaeger

The Department of Health and Human Services' Office for Civil Rights has officially kicked off its much anticipated second phase of audits of covered entities and their business associates. Required under the 2009 HITECH Act, the OCR must perform periodic audits of both covered entities—healthcare providers, health insurance plans, healthcare clearinghouses—and business associates for compliance with the Health Insurance Portability and Accountability Act's (HIPAA) privacy, security, and breach notification rules. The first phase was conducted as a pilot audit program in 2011 and 2012 on 115 covered entities.

The impetus behind the OCR's second phase of audits, which formally began on March 21, follows a scathing report issued in September 2015 by the HHS Office of Inspector General, which criticized the OCR for its lack of enforcement concerning compliance with HIPAA's privacy rule. In that report, the OIG determined that the OCR's oversight has been primarily reactive.

"It investigates possible non-compliance primarily in response to complaints," the report stated. "[the] OCR has not fully implemented the required audit program to proactively assess possible non-compliance from covered entities."

The findings from that report effectively put the OCR's feet to the fire "to be a bit more rigid during this phase than the last phase," says James Bowers, former vice president of corporate compliance for Aetna and now senior counsel at law firm Day Pitney.

On its website, the OCR described these audits as "primarily a compliance improvement activity." It warned, however, that it will not hesitate to initiate a full-blown compliance review if an audit report uncovers a "serious compliance issue," potentially resulting in significant fines and penalties. "There are certain core requirements of HIPAA that the OCR automatically will consider serious violations if they're not followed," says Eric Fader, a member of the life sciences and healthcare practice group at law firm Day Pitney.

One common compliance deficiency found during the pilot audits that often leads to an enforcement action by the OCR is failure to conduct an enterprise-wide risk assessment to ensure patients' health information is being adequately protected. "A risk assessment would uncover the types of omissions and shortcomings that audits are likely to be looking for," says Fader.

Many healthcare entities are still learning this lesson the hard way. Recently, for example, North Memorial Health Care of Minnesota, a non-profit health care system, reached a $1.55 million settlement with the OCR to resolve charges that it violated HIPAA's privacy and security rules by failing to enter into a business associate agreement with a major contractor and failing to institute an enterprise-wide risk analysis to address the risks and vulnerabilities to its patient information.

"Two major cornerstones of the HIPAA rules were overlooked by this entity," Jocelyn Samuels, director of the OCR, said in a statement. "Organizations must have in place compliant business associate agreements as well as an accurate and thorough risk analysis that addresses their enterprise-wide IT infrastructure." Other compliance measures the OCR will be looking for include whether covered entities have in place encryption capabilities; an up-to-date notice of privacy practices; a breach notification and response plan; and proper documentation of these measures.

In case compliance officers in the healthcare industry need one more reason to keep their HIPAA compliance program up-to-date and readily available, keep in mind that you will have only 10 business days to respond to an audit inquiry. "You can't cobble something together in 10 days that's going to pass muster if your program is weak or non-existent," says Dianne Bourque, a member in the health law practice at law firm Mintz Levin.

Audit preparation

Unlike the pilot audit program, the second audit phase focuses on both covered entities and their third-party affiliates, which generally include any business that provides a service to a covered healthcare entity and that receives protected health information in the course of providing that service. Business associates may include, for example, healthcare billing companies, Medicare payers, hospital management companies, and cloud computing companies that store protected health information.

"The first thing I would recommend to anyone right now is to develop an audit response plan," says Samuel Cohen, a senior associate in the healthcare practice at Arent Fox." For example, who is going to be in charge of responding? What frontline employees may need to be involved in getting documentation? You don't want an OCR notification letter to be the first time you've thought about these questions, he says.

During the first round of audits, the OCR will communicate with covered entities and business associates by e-mail to obtain and verify contact information. "There is no mercy from [the] OCR if the e-mail is filtered out into a spam folder," says Bourque. "You're on the hook for responding."

Once the OCR obtains that contact information, covered entities and business associates must then fill out a pre-audit questionnaire designed to gather data about their size, type, and operations. "Covered entities and business associates would be well served to have their audit response team ready and well-organized," says Reece Hirsch, a partner in the healthcare practice at Morgan Lewis. Develop a process to ensure audit response teams will be able to quickly gather and have easy access to the following pertinent documents:

» A list of the business associates, including their contact information and the nature of the services they provide;

- » A copy of your HIPAA privacy, security, and breach notification policy and procedures;
- » A copy of the findings from the latest enterprise-wide risk assessment;
- » Evidence of employee training on HIPAA privacy and security rules; and
- » A copy of an incident response plan concerning data breaches.

If a healthcare organization or business associate fails to respond to an initial e-mail or fails to provide adequate information during a pre-audit questionnaire, the OCR will then turn to publicly available information to create its audit pool. Failing to respond will not make you immune to a HIPAA compliance audit. The OCR said it will not audit entities, however, with an open complaint or that are currently undergoing an OCR compliance review.

Audit process

The first round of audits will be desk audits of covered entities followed by a second round of desk audits of business associates. All desk audits in this phase will be completed by the end of December 2016, the OCR said.

The third—and final—round of audits will be onsite, lasting three to five days, and will examine a broader scope of requirements from the HIPAA rules than desk audits. Although the OCR will conduct fewer onsite audits than the pilot phase, covered entities and business associates should be prepared for a site visit, nonetheless. "If the OCR decides to turn the onsite audit into a compliance review, that could be a cause for concern," says Leeann Habte, senior counsel in the healthcare practice at law firm Foley & Lardner.

"It's always a good idea to spot check," says Bourque. Not all HIPAA-covered entities and business associates may have the staff or time to conduct a mock audit, she adds, but you can still compare your current practices to the audit protocols published on the OCR's website by asking some key questions:

- » When was our last risk assessment? Are we due for another one?
- » Do we have easy access to our business associate agreements?
- » When was the last time we conducted employee training on HIPAA privacy, security, and breach notification rules?
- » Did everybody complete training? Do we have documentation to show that?
- » Where do we keep our incident log?

Following the audit—whether it's a desk or onsite audit—the OCR will produce a draft report, at which time the audited entity will have 10 days to review and respond with written comments. The final report will be completed by the OCR within 30 days and delivered to the audited entity.

With both desk audits and on-site audits, the OCR will not post a list of audited entities or the findings of an individual audit. Such information, however, may be subject to release under the Freedom of Information Act. "There is some danger of a sub-standard audit report getting into the hands of plaintiffs' counsel, thereby exposing organizations to private actions, as well as state attorney general actions," says Bowers.

Even if you are not selected for an audit, taking proactive measures to develop or reinforce your HIPAA privacy, security, and data breach response compliance program will help reduce the risk of an OCR enforcement action in the future. ■

OCR'S CURRENT AUDIT PROTOCOL

Below is a description from the Office of Civil Right's describing its current audit protocol.

The OCR HIPAA Audit program analyzes processes, controls, and policies of selected covered entities pursuant to the HITECH Act audit mandate. OCR established a comprehensive audit protocol that contains the requirements to be assessed through these performance audits.

The entire audit protocol is organized around modules, representing separate elements of privacy, security, and breach notification. The combination of these multiple requirements may vary based on the type of covered entity selected for review.

The audit protocol covers privacy rule requirements for:

- Notice of privacy practices for personal health information (PHI);
- Rights to request privacy protection for PHI;
- Access of individuals to PHI;
- Administrative requirements, uses, and disclosures of PHI;
- Amendment of PHI; and
- Accounting of disclosures.

The protocol covers security rule requirements for administrative, physical, and technical safeguards.

The protocol covers requirements for the breach notification rule. The protocol is available for public review and searchable by keyword(s) in [this] table.

Please be aware that the protocol has not yet been updated to reflect the Omnibus final rule, but a version reflecting the modifications will be available in the future.

Source: OCR.

Healthcare and Effective Cyber-Security Hygiene

You're a large healthcare provider that's having trouble accessing vital records in your hospital's computer network, IT has started an internal probe, and, worse, the attackers are demanding ransom to obtain the decryption key. How do you respond?

by Jaclyn Jaeger

Imagine this: You're a large healthcare provider whose staff is having trouble accessing vital records in your hospital's computer network. Your IT department begins an immediate investigation and determines the cause to be a malware attack. Worse yet, the attackers are demanding ransom to obtain the decryption key. How do you respond?

For Hollywood Presbyterian Medical Center, this was no fire drill. On Feb. 17, the hospital disclosed that it had experienced a malware attack earlier that month, which temporarily affected the operation of its computer network. Specifically, the malware locked access to certain computer systems by encrypting files, preventing hospital staff from sharing communications electronically.

To make matters worse, the hackers demanded ransom to obtain the decryption key—40 Bitcoins, or approximately $17,000, to be exact. "The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key," Hollywood Presbyterian Chief Executive Officer Allen Stefanek said in a statement. "In the best interest of restoring normal operations, we did this." The hospital said it also immediately notified law enforcement.

Hollywood Presbyterian is not alone. Cyber-attacks like ransomware—a specific form of malware designed to hold data hostage on infected systems until the owner pays the attacker a monetary reward—continue to plague the healthcare industry. According to a healthcare cyber-security survey conducted by KPMG, 81 percent of 223 U.S.-based healthcare executives polled said their organizations have been compromised by at least one cyber-attack during the past two years.

Furthermore, the survey results also showed that only half said they felt they are adequately prepared to prevent an attack. "The vulnerability of patient data at the nation's health plans and approximately 5,000 hospitals is on the rise, and healthcare executives are struggling to safeguard patient records," says Michael Ebert, leader of the healthcare and life sciences cyber-practice at KPMG.

It's also important to keep in mind, the cost of failing to prevent a cyber-attack goes far beyond operational expenses. Many companies incur additional costs associated with reputation and brand damage, loss of customers, revenue loss, loss of productivity, and credit monitoring services for employees or customers, and potentially even legal fees and regulatory fines and penalties associated with a data privacy and security breach.

> "The vulnerability of patient data at the nation's health plans and approximately 5,000 hospitals is on the rise, and healthcare executives are struggling to safeguard patient records."
>
> Michael Ebert, Leader of the Healthcare, LIfe Sciences Cyber Practice, KPMG

"We're not talking about spending a few hundred thousand dollars," says Ebert "We're talking about spending millions of dollars."

Other threats

In addition to ransomware, Distributor Denial-of-Service (DDoS) attacks are another evolving threat in the healthcare sector. DDoS attacks result when hackers command a fleet of remotely controlled computers to flood a targeted network with traffic, effectively bringing the network to its knees and resulting in long delays and several outages.

"What we're seeing this year, for the first time in several years, is that the top motivation is around criminal activity," says Gary Sockrider, principal security technologist at software company Arbor Networks. Similar to ransomware, DDoS attacks can involve extortion by hackers; if you don't pay a ransom, they'll keep the site down.

For many years, companies' attitudes concerning DDoS attacks has been, 'Yes, it's going to take us offline and it's a big pain and it can be costly, but at least we don't have to worry that our data is going to be lost,'" says Sockrider. Think again.

Increasingly, cyber-criminals are using DDoS attacks merely as a smokescreen to infiltrate the network with malware to steal data, such as intellectual property or personally identifiable information. "If you've been the victim of a DDoS attack, you should absolutely consider that an indicator of a compromise, and you should look to see if, and where, you've been compromised," Sockrider adds.

Such multivector attacks are much more difficult to defend. "It's like whack-a-mole," says Sockrider. As soon as you take care of one attack vector, another one rears its ugly head.

Security measures

Getting ahead of a cyber-attack means being one step ahead of the hackers. "It all boils down to leverage," says Peter Tran, lead worldwide cyber-defense practice, RSA. "He who holds the greatest leverage is most likely almost always going to win."

In the healthcare sector, in particular, cyber-attackers hold nearly all the leverage if the provider doesn't have any backup to the data. In Hollywood Presbyterian's case, for example, the hospital clearly did not have any kind of an effective recovery backup system.

Tran

"We're talking about a fundamental failure of IT security controls," says Ebert. "I've had clients who had breaches that never disclosed their ransomware, because they effectively were able to recover their environment."

Just having a backup recovery system in place, however, isn't the answer to all your problems. "Ransomware in the cloud is an emerging threat," says Tran. "Just because you're backing up your data in the cloud doesn't make you immune from your cloud backups also being held for ransom."

More often than not, the attacker will give the decryption key back once the ransom is paid, "but that doesn't mean the attacker doesn't have a secondary or third way to get back into the system again," warns Tran.

Reducing the threat of a cyber-attack comes down to good security hygiene, starting with employee security awareness training. "We have found that employees and hospitals are not that well trained on cyber-security," says Stu Sjouwerman, founder and CEO of KnowBe4, a security awareness training firm. "Bad guys go after low-hanging fruit. Low-hanging fruit is people."

Ransom, for example, is carried out when an employee clicks on an infected e-mail or an attachment. Once that device is infected with the ransomware, the files become encrypted. "It's still very easy to manipulate someone to opening up an infected attachment," says KnowBe4's Sjouwerman.

He recommends sending all employees frequent simulated phishing attacks to keep them on their toes. "That is where compliance and IT can work together," he says.

"IT security and compliance work hand-in-hand," Sjouwerman adds. "Being compliant doesn't necessarily mean you are secure."

Good security hygiene also means having in place a leader who is solely responsible for information security, says Ebert. Furthermore, whoever is leading your company's security efforts should have the resources and leverage to perform the job effectively, he says.

If your chief information security officer sits inside the technology department, says Ebert, how does that CISO report to compliance? How does that CISO understand the data security requirements that it needs to execute?

By converging compliance, audit, and legal with information technology and security, you can gain a 360-degree view of the situation in the event of an attack, says Tran. It's also essential to identify where your most valuable data resides and put continuous monitoring controls around those systems.

"We've got the technology," concludes Ebert. "We need the right resources, and we need the right understanding of how to address the weaknesses." ■

HEALTHCARE SURVEY RESULTS

Below is an excerpt from KPMG's healthcare and cyber-security survey.

With the changing nature, depth and consequences of cyber-attacks in healthcare, the nature of preventing, monitoring and managing those threats requires a new approach, based on:

Incorporation of cyber-security in the technology and network architecture upfront, via strategic design. Since many organizations achieved their interconnectivity by evolution, resulting in inadequate controls, what is in many cases required today is a redesign and development of a security implementation plan. Investment in security needs to become part of a cohesive, coordinated digital strategy.

A well-prepared and coordinated cyber security team and a security operations center. A successful approach requires appointing an executive with sole responsibility over cyber security, as well as capabilities for instant monitoring. Other areas that need to be covered include managing the breach itself and communicating with various constituencies.

Increased cyber-security awareness and capabilities at all levels. Cyber security is a business risk as well as a technology risk. Thus cyber security executives need to be equally conversant in both. While the executive involvement typically boils down to the awareness component, it is important to have board members savvy about cyber security and able to help management in this area.

Taking a broad view of the organization when implementing cyber security. By working with a variety of business partners, organizations have, in effect, become extended value chains. The third-party vector poses an increased cyber-security risk. It is crucial to understand the inherent risk of having multiple third-parties engaged and to identify risks that have to be remediated.

Source: KPMG.

Compliance Lessons in the Healthcare Sector

by Jaclyn Jaeger

As a healthcare or life sciences company, perhaps you've never been in trouble with the Department of Health and Human Services—and perhaps you never will—but it would be a mistake to overlook the important compliance lessons learned by those who have, lest you suffer the same fate.

When enforcement actions against healthcare or life sciences companies arise, many choose to settle their cases prior to litigation, often resulting in a corporate integrity agreement (CIA) with the Department of Health and Human Services Office of Inspector General (HHS-OIG) to avoid exclusion from federal healthcare programs. CIAs generally impose compliance obligations on companies with the intent to prevent future misconduct.

By carefully scrutinizing these agreements, compliance and audit teams in the healthcare and life sciences industries can get a better sense of where to focus their own efforts. "Typically, you don't find out exactly what the government wants until after the fact," says Sarah Crotts, an associate with law firm Wall Babcock. "It's always good to keep an eye out to see what the government is requiring of similarly situated entities."

And companies have no shortage of guidance: As of February, the HHS-OIG had 216 open CIAs, including 12 involving amendments to prior agreements, according to data on the agency's website. The number of CIAs over the last five years has fluctuated from a low of 35 in 2012 to a high of 53 in 2015. To date, only one CIA has been reached in 2016.

Although HHS-OIG tailors each CIA to address the specific facts of each case, they all require the following seven core elements of a compliance program under the U.S. Sentencing Guidelines:

- Designation of a compliance officer and compliance committee;
- Written policies and procedures;
- Comprehensive employee training and education;
- Effective and open lines of communication;
- Consistent enforcement of standards as demonstrated by disciplinary action;
- Auditing and monitoring to detect misconduct; and
- Developing corrective action initiatives.

Beyond these baseline compliance obligations, many of the provisions included in these CIAs are industry-focused. Settlements pertaining to pharmaceutical companies, for example, now typically demand stringent and widespread monitoring obligations.

"Those requirements can be quite onerous on an entity," says Crotts. "It adds a level of scrutiny that we haven't really seen before."

For example, under separate CIAs with Switzerland-based pharmaceutical giant Novartis and U.S.-based healthcare giant Abbott Laboratories, both companies must formally establish a comprehensive "Field Force Monitoring Program" (FFMP) to evaluate and monitor their sales representatives' interactions with healthcare professionals and healthcare companies to identify potential off-label promotional activities or other misconduct. This includes the review of records relating to these interactions, a speaker monitoring program, and direct field observations of sales reps.

In May 2012, Abbott Labs pleaded guilty and agreed to pay $1.5 billion to resolve criminal and civil liability arising from the company's unlawful promotion of its prescription drug Depakote for uses not approved by the Food and Drug Administration. The terms of the CIA will expire in 2017.

Novartis' CIA, which would have expired last year, has been amended and extended for an additional five years as part of a $370 million settlement reached with the Justice Department in November 2015 to resolve allegations that the company paid kickbacks—in the form of patient referrals and rebates—to specialty pharmacies in exchange for those pharmacies recommending Novartis drugs.

Board Oversight

Another emerging development in recent CIAs is the increasingly expanding scope of compliance obligations imposed on boards of directors and management. Although the compliance obligations demanded by many CIAs are not new, "they're being refined to assure greater focus on the accountability provisions for management and the board," says Kathleen McDermott, a partner with law firm Morgan Lewis.

In that context, boards of directors are now often required to review and oversee matters related to compliance with both federal healthcare laws and obligations imposed under the CIA, "so it gives the board a direct role in compliance," says McDermott. Additionally, many CIAs require that each member of the board receive training regarding these responsibilities, and further provide written certification that the company meets the requirements of an effective compliance program.

For example, healthcare services company Kindred Healthcare and RehabCare Group last month entered into a five-year CIA that requires the board to meet at least quarterly to review and oversee Kindred's compliance program for RehabCare, "including but not limited to the performance of the compliance officer and compliance committee," the CIA states.

CIAs also now commonly require that the board hire an outside compliance expert with knowledge of federal healthcare programs to assist the board in reviewing the effectiveness of the company's compliance program. Such a provision is included in CIAs reached with Novartis and Millennium Health.

Increasingly, too, HHS-OIG through the force of CIAs is imposing greater accountability on management. The Novartis CIA, for example, requires that any employee at the vice president level and higher—more than two dozen executives in all—monitor and oversee activities within their areas of authority, and annually certify that the applicable business unit is in compliance with healthcare laws and the CIA.

A similar provision was included in a CIA that Tuomey Healthcare System reached with the government in October 2015. That CIA, along with a $237 million judgment, resolved allegations that Tuomey illegally billed Medicare for services referred by physicians with whom the hospital had improper financial relationships.

From the HHS-OIG's standpoint, expanding the scope of managers who must certify compliance will help not only mitigate abuses of federal healthcare laws, but also make directly accountable those who are in a position to prevent, uncover, correct, or report misconduct.

CIA Negotiations

McDermott says another "notable trend" in recent settlements is that some companies have resolved civil fraud matters without getting a CIA. "That's a very good sign that the OIG is not indiscriminately imposing CIAs on companies that have demonstrated they have sufficient compliance program safeguards," she says.

Examples include Teva Pharmaceuticals' $27.6 million settlement reached with the Justice Department in May 2014, and medical-device company C.R. Bard's $48.2 million settlement reached in May 2013. Both cases resolved violations of the False Claims Act.

In some cases, a corporate parent also may be able to evade a CIA in situations where the wrongdoing was confined to a subsidiary or operating division of the corporate parent. In those cases, during CIA negotiations, the HHS-OIG will closely scrutinize where authority resides within the company.

These investigations frequently go on for years, over which time the company may have gone through significant changes, "such that it's simply not the same organization with the same people," says McDermott. Compliance enhancements may have been sufficiently implemented that negate the need for government oversight, she says.

The costs alone are reason enough to negotiate the terms of a CIA. "Even those with robust compliance programs still incur a great deal of training and auditing costs to ensure timely compliance," says McDermott. The repercussions for breaching a CIA can be even more severe, with the worst case scenario being a bar from participating in federal health care programs.

"CIAs, in general, place the company under a lot of scrutiny," says Crotts. The time, and effort, and staffing—including the reallocation of responsibilities, in many instances—that it takes to simply comply with CIA, can be daunting.

At the inception of a subpoena or that the beginning of an investigation, McDermott recommends that the company and their counsel should contemplate not only how to respond to an investigation, but also be thinking about the overall health of the compliance program: "Is it effective? If you're thinking about that at the end of the investigation when you're talking about a resolution, that's a little too late."

Corporate integrity agreements are one of many valuable resources companies have to better understand what the government considers to be a robust compliance program. As such, companies in the healthcare and life sciences industries should continually review new CIAs as part of their annual risk assessment. ■

FIELD FORCE MONITORING & REVIEW EFFORTS

Below is an excerpt from the original corporate integrity agreement that Novartis Pharmaceuticals entered into with the DoJ in 2010.

To the extent not already accomplished, within 120 days after the Effective Date, Novartis shall establish a comprehensive Field Force Monitoring Program (FFMP) to evaluate and monitor its sales representatives' interactions with HCPs and HCIs. The FFMP shall be a formalized process designed to directly and indirectly observe the appropriateness of sales representatives' interactions with HCPs and HCIs and to identify potential off-label promotional activities or other improper conduct. As described in more detail below, the FFMP shall include: (1) a Speaker Monitoring Program; (2) direct field observations (Observations) of sales representatives; and (3) the monitoring and review of other records relating to sales representatives' interactions with HCPs and HCIs (Records Reviews).

Prior to the Effective Date, Novartis had systems to address detailing, sampling, and medical inquiries. The detailing systems shall continue to include controls designed to ensure compliance with Federal health care program and FDA requirements and shall permit the tracking of detailing-related activities, including the submission of Inquiries (as defined above in Section III.B.2.g) and the distribution of samples of Government Reimbursed Products to HCPs. The detailing systems shall continue to include centralized mechanisms through which sales representatives may submit Inquiries to Medical Affairs. With regard to the distribution of samples, the detailing systems and its controls shall prevent the delivery of samples of particular Government Reimbursed Products to HCPs that Novartis has identified as belonging to a specialty group that is unlikely to prescribe the particular Government Reimbursed Product for a use consistent with the FDA-approved label for the product.

Speaker Program Activities. With regard to speaker programs, Novartis shall maintain processes to require all speakers to complete training and enter written agreements that describe the scope of work to be performed, the speaker fees to be paid, and compliance obligations for the speakers (including requirements that the speaker may only use Novartis approved materials and may not directly or indirectly promote the product for off-label uses.) Novartis shall maintain centralized processes and related electronic systems through which all speaker programs are tracked. This system shall establish controls regarding eligibility and qualifications of speakers and venues for the programs, Novartis shall ensure that speakers are paid and tracked according to a centrally managed process, and using a pre-set rate structure determined based on a fair-market value analysis conducted by Novartis.

Novartis shall maintain a comprehensive list of speaker program attendees through its centralized system. In addition, Novartis shall track and review the aggregate amount (including speaker fees, travel, and other expenses) paid to each speaker in connection with speaker programs conducted during each Reporting Period ...

Source: Justice Department.

Risk management: an ounce of prevention is worth a pound of cure

By RSA

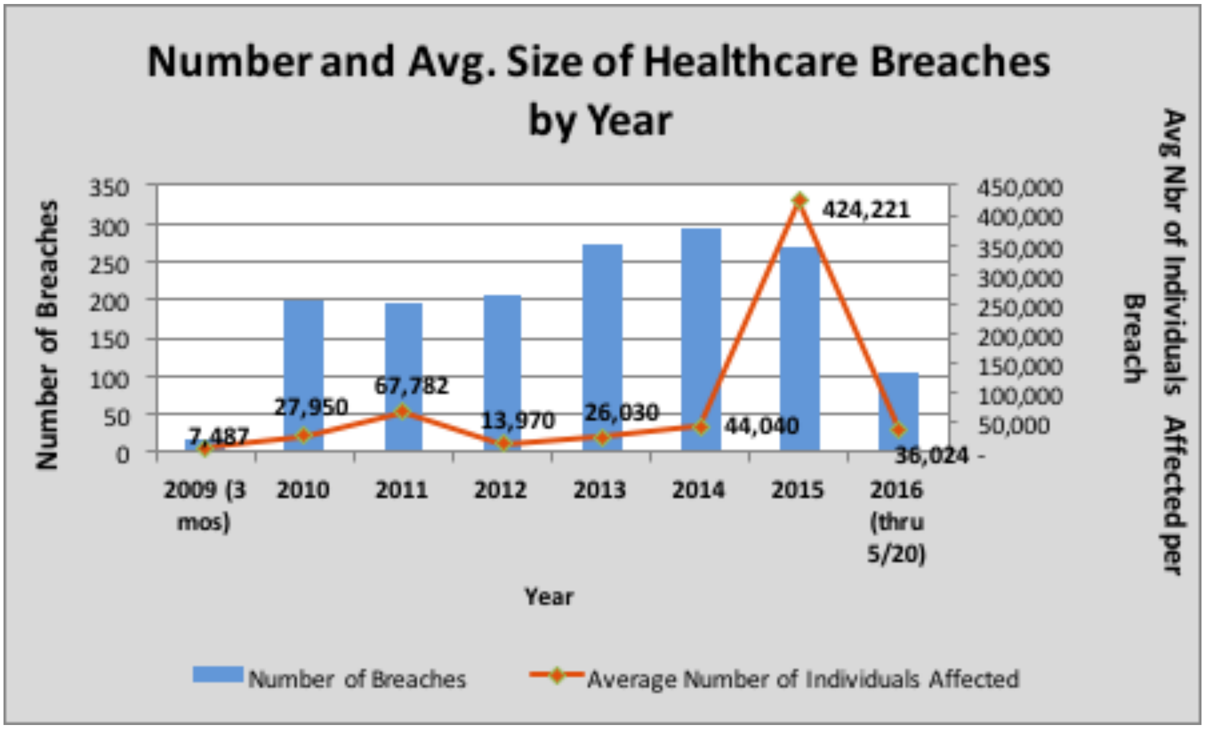
When talking about someone's health, how many times have you heard the saying, "An ounce of prevention is worth a pound of cure"? In this day and age, the saying is no less true for healthcare providers than for the subject of healthcare. Hospitals, clinics, physician's offices, and providers of products and services to healthcare, such as wholesale and retail pharmaceutical providers, medical device manufacturers, and billing and recordkeeping providers have grown in complexity and face previously unforeseen risks and regulatory burdens. These risks and regulatory obligations are significant, in some cases threatening the very existence and mission of healthcare providers.

In this e-Book we explore some common and emerging risks facing healthcare organizations today, and how RSA Archer's governance, risk and compliance (GRC) solutions can help organizations more proactively manage the ills that could befall them.

Issues Management

Management issues arise almost at the outset of the creation of any organization, including healthcare organizations. Operational deficiencies, missing policies and procedures, and incomplete tasks needed to achieve objectives are all issues that must be addressed by management. Recommendations from internal and external auditors, consultants, and regulatory agencies, such as the Office of Inspector General and Office for Civil Rights, all demand management attention within defined timeframes. In many organizations there can be so many issues that it is difficult to track and manage them using traditional means. Different lists of issues get scattered throughout the organization with no centralized system of record. No prioritization exists, accountability for issue remediation does not exist, and mechanisms do not exist to ensure that remediation plans and tasks are being addressed in a timely manner in accordance with

Figure 1



the commitments that have been made.

With RSA Archer Issues Management you can capture any risk or compliance-related issue, including risks that exceed acceptable levels; failed or deficient controls; key indicators outside boundaries; and loss events or incidents requiring remedial actions. RSA Archer Issues Management enables healthcare organizations to catalog their internal and external audit findings, regulatory examination issues, and management-identified issues; establish accountability for problem resolution; and track remediation plans against commitments and due dates. Robust reporting makes it easy for all levels of management and the board to understand the full scope of outstanding issues, priorities, and remediation timelines.

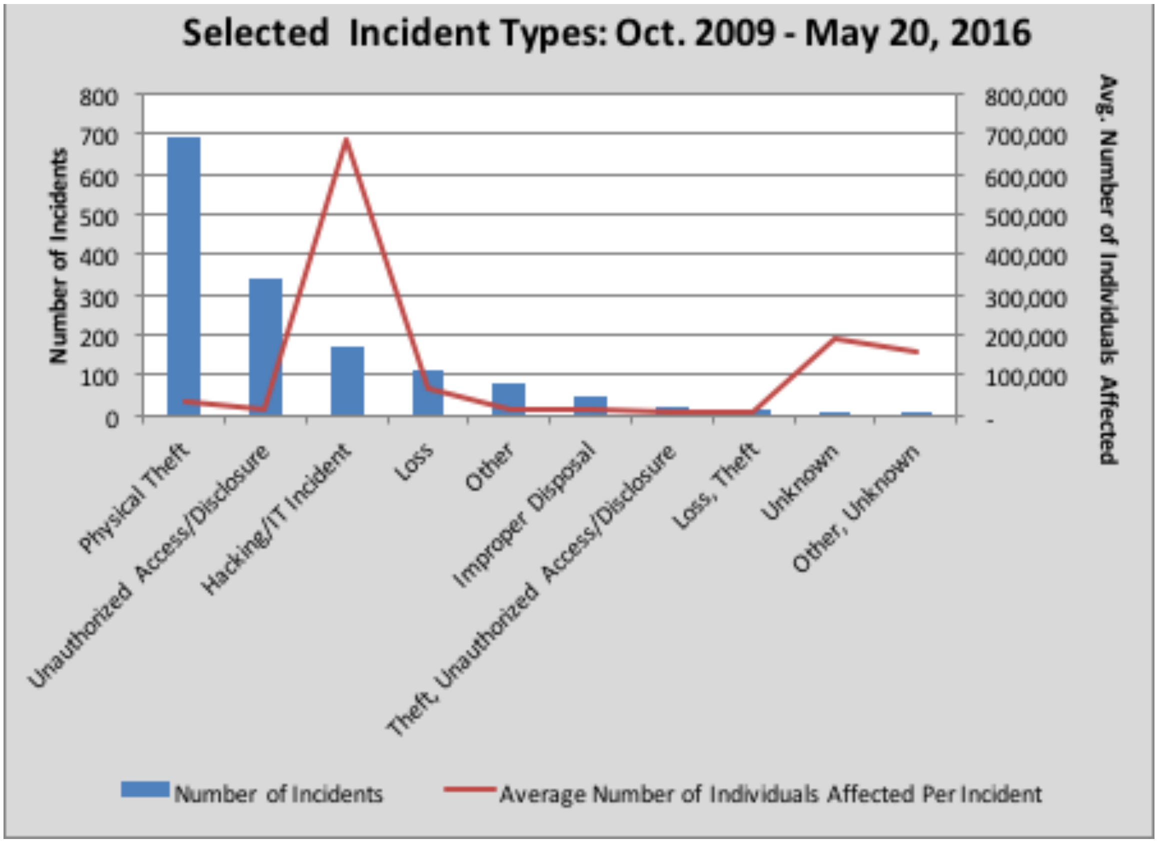
Information Security

In the *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data* conducted by Ponemon Institute, Ponemon reported that "89% of healthcare organizations and 60% of business associates (a.k.a. third parties or vendors) experienced data breaches over the past two years. 79% of healthcare organizations experienced multiple data breaches (two or more) in the past two years—up 20% since 2010."

Entities covered by the Health Insurance Portability and Accountability Act (HIPAA) and their business associates are required to provide notifications following a breach of unsecured protected health information affecting 500 or more individuals. The U.S. Department of Health and Human Services – Office for Civil Rights (OCR) maintains a website that lists all of the breach notifications they have received (https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf). Between October 2009 and May 2016, over 1,539 breaches have been reported affecting over 158 million individuals. All of the data from this website is exportable, =so some interesting analysis can be performed.

Figure 1 depicts the number of breach reports received each year affecting more than 500 individuals, and it shows the average number of individuals affected in a breach for each reporting year. The average number of individuals affected by a breach skyrocketed in 2015 due to three reported breaches affecting more than 75 million individuals each! Excluding these very large breaches, the average number of individuals affected in 2015 was approximately 51,000. From 2012 to 2015, excluding the large breaches in 2015, the average number of individuals affected per

Figure 2



breach increased at a rate of 57%.

In 2015, Ponemon estimated that the average cost of a healthcare breach was $363 per exposed personally identifiable record. Extrapolating this cost to these numbers above, the cost of an average breach is in excess of $18 million. That is a staggering number for most healthcare providers.

Examination of the largest types of breaches reported (Figure 2) reveals a few interesting findings:

(1) The largest number of breaches relate to the physical theft of information. Although the number of individuals affected is relatively low, physical control of information is a prevalent problem;

(2) Cyber-attacks result in the largest average number of individuals being affected; and

(3) Some organizations are unable to ascertain the source of breaches when they are discovered.

Effectively managing information security risk is one of many issues of prime importance to healthcare organizations.

The most frequent source of protected health information breach comes from unauthorized physical access (theft). The risk of physical theft of information requires organizations to establish policies and procedures for the proper storage, management, and destruction of physical records and for physical access to systems that contain electronic records, such as unsecured laptop computers that contain protected health information (PHI). The policies and procedures have to be effectively communicated to employees and business associates and are often further codified within a formal code of conduct. For large healthcare organizations, it is impractical to manually maintain and deliver physical security policies and procedures.

With RSA Archer, organizations can document their information security policies and procedures, manage the lifecycle of policy and procedures, including the approval and reaffirmation of policies and procedures, and the delivery and affirmation of the policies, procedures, and code of conduct by employees and business associates.

Cyber-attacks on healthcare firms result in the largest breaches of protected health information, ranging on average from 50,000 PHI records to tens of millions of records. Malicious cyber-attacks are often targeted to exploit the identity of patient records. Recently, cyber-attacks have taken the form of "ransomware" where the cyber-attacker locks a healthcare provider's computer systems and records until the provider pays a ransom.

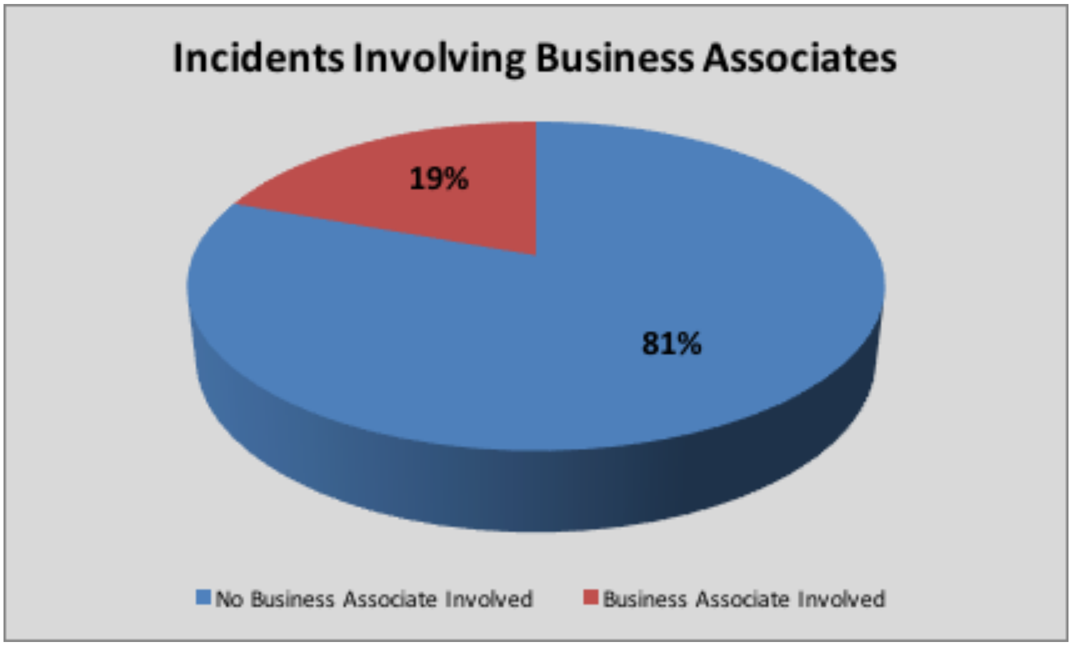
To minimize the risks associated with cyber-attacks, healthcare organizations must work toward better understanding and management of their electronic information infrastructure, and create a mechanism to rapidly identify, respond to, and mitigate the impact of any cyber-incident, when one occurs.

RSA Archer IT & Security Risk Management allows you to determine which assets are critical to your business, establish and communicate security policies and standards, detect and respond to attacks, identify and remediate security deficiencies, and establish clear IT risk management best practices.

The source of a number of breaches reported to the OCR could not be accurately determined and were reported as unknown. For information security managers, there are few things more frustrating than knowing that your organization has been breached but not knowing how. Learning how incidents occur is critical to conducting the root-cause analysis necessary to initiate corrective action to prevent similar breaches in the future.

Visibility across your technology infrastructure is critical to prevent, detect, and manage information security breaches. RSA enables you to combine the workflow and business context from RSA Archer with the deep log and packet inspection and

Figure 3



forensics of RSA Security Analytics giving you the actionable information to identify active threats and take corrective steps to mitigate similar future events.

Much is being written today about the risk of Internet-connected medical devices becoming part of the "Internet of Things" (IoT). The use of IoT medical devices is growing within the healthcare industry and the Food and Drug Administration is beginning to take notice that patient safety could be seriously compromised if security issues are not managed throughout the lifecycle of these medical devices. Healthcare organizations are expected to have an inventory of their IoT devices and be actively managing them to ensure they operate as expected, that security patches are being applied in a timely manner, and that unauthorized access is adequately prevented.

RSA Archer can help you manage your IoT medical devices by giving you a centralized location to catalog devices and set up governance processes to capture new devices before they are placed into service. In addition, you can monitor the timeliness of your security patch management and document, test, and monitor controls around access to the devices.

Third Party Governance

The last analysis worth mentioning is an examination of the involvement of business associates in information security breaches. As mentioned earlier, Ponemon reported that 60% of business associates have experienced data breaches over the past two years. In the incidents reported to OCR (Figure 3), you can see that 19% of all breaches impacting more than 500 individuals involved business associates. In general, healthcare organizations have an obligation to ensure that the business associates they use are engaged with properly crafted legal contracts and that business associates have sound security procedures in place.

The OCR has begun to aggressively fine organizations whose business associates are involved in breaches but have been operating without adequate, formal HIPAA business associate agreements. For example, in March 2016, the OCR settled its investigation of a hospital and clinic system in Minnesota for $1.55 million after learning that the organization had been sharing a large amount of PHI with a business associate without having a business associate agreement in place. The OCR became focused on the problem after the organization reported a loss of PHI on a stolen laptop of a business associate employee.

Effectively managing business associate relationships requires a methodical approach to capture new and existing relationships to ensure that all required contractual documents are in place, that the risks and controls related to the business associate are well understood, and that the business associate is performing up to expectations.

With RSA Archer Third Party Governance, you can capture prospective relationships, engage affected stakeholders, and assess contract risk, financial wherewithal, and inherent and residual risks across multiple risk categories, including a business associate's information security practices. This enforces risk-based selection and ongoing management and establishes performance metrics. RSA Archer Third Party Governance automates and streamlines oversight of your business associate relationships by facilitating key activities necessary to fulfill regulatory obligations and best practices across the entire business associate lifecycle.

Business Resiliency

Many healthcare facilities have chosen to offer 24/7 services as a result of regulatory obligations, such as to fulfill Medicare Conditions of Participation (CoP), to be more competitive or to utilize capital investments more efficiently. Whatever the reason, maintaining uninterrupted services can be a significant challenge. Threats to business resiliency arise in many ways including: Acts of God; cyber-attacks that result in ransomware; errors or malicious attacks by employees and third parties, including utility companies accidentally cutting power and communication feeds; or business interruptions that can result from an interruption of service delivery by business associates.

Effective business resiliency management means taking steps to prevent service interruptions and practicing for those inevitable events to minimize the impact of interruptions when they occur. Both tasks require you to identify likely scenarios, engage management and staff in preventing and preparing for interruptions, and knowing how to respond quickly when an interruption does occur.

RSA Archer Business Resiliency provides an automated approach to business continuity and disaster recovery planning and execution, enabling swift response in crisis situations to protect your ongoing operations. With RSA Archer, you can assess the criticality of business processes and supporting technologies, and develop detailed business continuity and disaster recovery plans using an automated workflow for plan testing and approval. Key dashboards and reports provide visibility for your senior management, giving them a better understanding of continuity risks, insight into budget requirements, and a level of confidence that a solid resiliency program is in place if a crisis occurs.

Summary

Every healthcare organization faces a myriad of risks to its mission. These risks include:

- Patient safety
- Complying with laws and regulations
- Information security
- Business associates
- Business resiliency

The growing scope and complexity of these risks make it quite challenging to effectively manage risk and compliance issues. Some risks are too large for organizations to wait until something bad happens; they must take a proactive stance to be most effective. They have to understand the growing complexity of risk and have confidence that the risks are being adequately managed to ensure objectives are going to be fulfilled. It is no longer practical to gain such understanding using pencil, paper, spreadsheets, and MS Word documents. More methodical and sustainable governance is needed. With RSA solutions, you can master the risk and compliance landscape, fulfilling the adage, an ounce of prevention is worth a pound of cure. ■

Connected Medical Systems, HIPAA Audits Coming

Inspectors at the Department of Health & Human Services are going to be studying the security protocols for medical devices and electronic health records, which means CCOs in healthcare should make sure policies & controls can pass muster

by Jaclyn Jaeger

Greater scrutiny over the security for medical devices and electronic health records are just two of the new priorities for the Office of Inspector General for the Department of Health and Human Services, according to its work plan for fiscal 2016.

The plan, published earlier, offers hospitals, medical practices, nursing facilities, drug makers, and medical device makers a glimpse into where regulators will focus their attention in the coming year—and thus, where compliance officers and internal auditors should focus their risk management and internal auditing efforts.

“The work plan can show new areas that the OIG has identified as emerging risks, or it can provide a window into what areas the OIG will focus on based on the data analytics the OIG has been doing,” says Tony Maida, a partner in the law firm McDermott, Will & Emery. At the least, the work plan gives the healthcare and pharmaceutical industries a sense of how to set their own internal audit programs, he says.

The OIG said in its work plan that its “largest body of work” involves investigating matters related to Medicare and Medicaid, such as billing for services not rendered or medically unnecessary and services. Other hot topics include off-label marketing of prescription drugs and the solicitation and receipt of kickbacks, according to its work plan.

One brand new priority in 2016: a review the Food and Drug Administration’s oversight of medical devices networked to electronic health records (EHRs). “We will examine whether FDA’s oversight of hospitals’ networked medical devices is sufficient to effectively protect associated electronic protected health information (ePHI) and ensure beneficiary safety,” the OIG said in its work plan.

Medical devices—dialysis machines, radiology systems, and medication dispensing systems, for example—that are integrated with electronic medical records and the larger health network “pose a growing threat to the security and privacy of personal health information,” the OIG said. “Such

HHS-OIG FY 2016 WORK PLAN

Below, the OIC details what agencies it reviews during a public health inspection and what is the agency’s primary focus.

Hospitals’ electronic health record system contingency plans

We will determine the extent to which hospitals comply with contingency planning requirements of the Health Insurance Portability and Accountability Act (HIPAA).We will also compare hospitals’ contingency plans with government- and industry-recommended practices. The HIPAA Security Rule requires covered entities to have a contingency plan that establishes policies and procedures for responding to an emergency or other occurrence that damages systems that contain protected health information.

Controls over networked medical devices at hospitals

We will examine whether FDA’s oversight of hospitals’ networked medical devices is sufficient to effectively protect associated electronic protected health information (ePHI) and ensure beneficiary safety. Computerized medical devices, such as dialysis machines, radiology systems, and medication dispensing systems that are integrated with electronic medical records (EMRs) and the larger health network, pose a growing threat to the security and privacy of personal health information. Such medical devices use hardware, software, and networks to monitor a patient’s medical status and transmit and receive related data using wired or wireless communications. Medical device manufacturers provide Manufacturer Disclosure Statement for Medical Device Security (MDS2) forms to assist health care providers in assessing the vulnerability and risks associated with ePHI that is transmitted or maintained by a medical device.

Office for Civil Rights’ oversight of the security of electronic protected health information

We will determine the adequacy of the Office for Civil Rights (OCR) oversight over the security of electronic protected health information (ePHI). Prior OIG audits reported that OCR had not assessed the risks, established priorities, or implemented controls for its HITECH Act requirement to provide for periodic audits of covered entities and business associates to ensure compliance with HITECH Act and HIPAA Rule requirements and, therefore, had limited assurance that covered entities and business associates adequately protected ePHI. Prior OIG audits have also summarized numerous vulnerabilities in the systems and controls to protect ePHI at selected covered entities.

Source: OIG.

medical devices use hardware, software, and networks to monitor a patient's medical status and transmit and receive related data using wired or wireless communications."

Compliance officers at healthcare providers and medical device makers should be aware that handing over enforcement authority to the FDA marks a shift in authority from the OIG's fiscal year 2015 work plan, when the Centers for Medicare & Medicaid Services had oversight authority of medical devices networked to EHRs.

> "The work plan can show new areas that the OIG has identified as emerging risks, or it can provide a window into what areas the OIG will focus on based on the data analytics OIG has been doing."
>
> Tony Maida, Partner, McDermott, Will & Emery

"The FDA is actively working to ensure a collaborative approach to addressing medical device cyber-security across all stakeholders, including researchers, manufacturers, government, and healthcare facilities," says Angela Stark, a spokesperson for the FDA. "The FDA encourages these stakeholders to work together to openly identify challenges and discuss strategies and best practices for addressing medical device cyber-security in order to protect patient safety and promote public health."

As more wireless devices become integrated into healthcare systems, "providers and manufacturers have to be really diligent about making sure their systems are secure," says Nathan Kottkamp, a partner with law firm McGuire Woods.

The OIG also said it will step up its review of how the Office for Civil Rights oversees the security of ePHI. (OCR is the agency responsible for policing the privacy and security requirements of the Health Insurance Portability and Accountability Act.)

According to the OIG, previous audits found that OCR "had not assessed the risks, established priorities, or implemented controls" required under the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act. HITECH requires periodic audits of compliance with HIPAA's privacy, security, and breach notification rules.

Such gaps in oversight provided "limited assurance" that businesses and third parties were adequately keeping ePHI secure, the OIG said. Previous audits also found "numerous vulnerabilities in the systems and controls to protect ePHI at selected covered entities," the work plan said.

From a practical standpoint, depending on what the OIG's review finds, "it may influence OCR's activities going forward," Maida says. "It may result in OCR pursuing more cases."

HIPAA Audits

The OIG said it also plans to determine the extent to which hospitals comply with contingency planning requirements of HIPAA. The HIPAA Security Rule requires covered entities (such as hospitals) to have a contingency plan that establishes policies and procedures for responding to an emergency or adverse event that damages systems containing protected health information.

Even though hospitals must have a contingency plan in place, the HIPAA Security Rule doesn't specify what that contingency plan should look like. "It's hard to know what is deemed to be acceptable," Kottkamp says.

Healthcare providers would be well served to take a look at other industry-recognized standards and best practices, such as those used by the financial services industry, Kottkamp says. He further recommends that healthcare companies test those disaster relief plans: "Have you done a real-life fire drill where you shut down access to your main servers? If so, what backup information is available? How long does it take to retrieve?"

Also in 2016, healthcare organizations can expect more enforcement actions as the Department of Health and Huuman Services prepares to launch its new HIPAA compliance audit program.

HHS launched a pilot audit program in 2012, carried out by KPMG, which under contract with HHS conducted reviews of HIPAA compliance at 115 covered entities. "HIPAA audits were supposed to start sometime in 2015, but they were delayed," Kottkamp says. "My guess is that they're not going to start until 2016."

The HIPAA compliance audit program took a step forward in September, when government services firm FCi Federal announced that it had been awarded a contract to provide HIPAA auditing services to support HHS. FCi Federal said the $1 million contract was awarded for an 18-month performance period.

"This is the first task order granted on this contract to provide support to 13 nationwide HHS-OCR offices in the areas of monitoring, investigation, and enforcement of anti-discrimination and privacy laws; health information protection; and civil rights policy development, planning, education, and outreach," the company said in a statement.

Overall Enforcement Trends

Enforcement efforts against fraud in the healthcare industry show no signs of abating. For fiscal year 2015 (which ended on Sept. 30), the OIG reported expected recoveries of more than $3 billion, consisting of nearly $1.13 billion in audit receivables and $2.2 billion in investigative receivables, according to the work plan.

The work plan also reported exclusions of 4,112 individuals and entities from participation in federal healthcare programs in 2015; 925 criminal actions against individuals or entities that engaged in crimes against HHS programs; and 682 civil actions.

The numbers alone make enforcement efforts a lucrative activity for the government, and all signs are that HHS will continue to expand its caseload. ■

Managing Cyber-Risk in the Healthcare Industry

Recent high-profile data breaches at several major healthcare providers have jolted the industry, which is trying to piece together better ways to manage the risks

by Jaclyn Jaeger

Compliance officers in the healthcare industry should be revamping their cyber-security practices, following a surge in data breaches and the emergence of new cyber-threats that most healthcare organizations are still ill-equipped to address.

In 2015, hackers in China infiltrated the computer system of health insurer Anthem, stealing 78.8 million records containing protected health information (PHI) and other sensitive data, making it the largest data breach to ever hit the U.S. healthcare industry. It also marked the first state-sponsored cyber-attack of several that occurred in 2015.

In the second largest cyber-attack targeting the healthcare industry this year, health insurer Premera announced in March that Chinese hackers had gained unauthorized access to its systems, stealing 11 million records containing PHI.

> "As opposed to an organization trying to invest more money in firewalls or other types of technical solutions to protect against an intrusion, at this point you almost have to assume your network has already been breached"
>
> Rick Kam, President, ID Experts

The advanced nature of state-sponsored attacks makes them especially difficult to uncover. Premera, for example, said it discovered its cyber-attack in January 2015, almost nine months after the initial attack occurred in May 2014. In another example, health insurance company Excellus, which made headlines this year for suffering the third largest cyber-attack in the healthcare industry for affecting 10 million records, concluded that its breach occurred as early as December 2013.

The Anthem, Premera, and Excellus breaches are only the tip of the iceberg. According to data compiled from the HHS' Office of Civil Rights, 249 data breaches affecting 500 or more individuals occurred in 2015, resulting in the breach of 113.2 million total records. Of that amount, 56 were caused by a hacking incident.

Because of the widespread use of electronic health records (EHR) today, hackers are able to access individuals' personal information, credit information, and protected health information (PHI) all in one place, which translates into a high financial payout for any medical record sold on the black market.

According to the Federal Bureau of Investigation, cybercriminals are selling such information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHRs can then be used for such criminal activity as identity theft, filing fraudulent insurance claims, or obtaining prescription drugs illegally.

Vulnerabilities Persist

Despite healthcare organizations being a lucrative and easily vulnerable target for hackers, the healthcare sector is "not as resilient to cyber-intrusions compared to the financial and retail sectors," the FBI warned in a notice issued last year to healthcare providers. Such vulnerabilities further increase the risk of a cyber-attack.

In fact, cyber-attacks in the healthcare industry have increased 125 percent since 2010, according to a healthcare breach report conducted this year by the Ponemon Institute. The most vulnerable targets include hospitals, clinics, healthcare providers, and their "business associates (BAs)," which the Department of Health and Human Services (HHS) defines as a person or entity that performs services for a healthcare provider—such as patient billing firms, health plans, claims processing, and cloud services—involving the use or disclosure of PHI.

According to the report, the majority of healthcare organizations and BAs lack the funds and resources needed to protect patient data and are unprepared to meet the changing cyber-threat environment. Specifically, of the 90 healthcare organizations and 88 BAs polled, only 33 percent of healthcare organizations and 41 percent of BAs said they have sufficient resources to prevent or quickly detect a data breach.

The cost of not investing in effective privacy and security controls is a staggering $6 billion annually, with the average economic impact amounting to $2.1 million per healthcare organization, according to Ponemon figures. Even more telling is the fact that more than 90 percent of healthcare organizations said they experienced at least one data breach, with 40 percent experiencing more than five data breaches over the past two years.

Cyber-Security Measures

High-profile attacks like the ones that targeted Anthem and Premera—and even low-profile attacks that affect only a few individuals—should serve as a wake-up call to healthcare organizations to enhance their cyber-security efforts.

When working with your EHR and health IT developers, the Office of the National Coordinator Health Information Technology recommends asking the following questions to help understand their privacy and security practices:

» When my health IT developer installs its software for my practice, does its implementation process address security features such as encryption, auditing functions, backup and recovery routines, strong passwords, and more?

- Will the health IT developer train my staff on the above features so my team can update and configure these features as needed?
- How much of my health IT developer's training covers privacy and security awareness, requirements, and functions?
- How does my backup and recovery system work? Where is the documentation? Where are the backups stored? How often do I test this recovery system?
- How much remote access will the health IT developer have to my system to provide support and other services? How will this remote access be secured?

Understanding the location of your sensitive data and putting security controls around it—such as data encryption, limiting network access to that data, and having in place an early alert system—are good starting points, says Jason Rebholz, principal consultant at cyber-security firm Mandiant.

Network segmentation also helps thwart a cyber-attack, as does securing accounts with strong passwords and changing them regularly. You also want to have someone with the technical expertise to be able to identify the scope of the compromise and what data is potentially at risk, Rebholz adds.

Incident Response Plan

Being well-prepared to respond to a data breach means having a response team in place before a breach even occurs, conducting a mock cyber-attack to test the preparedness of your team, and having partners and vendors on call to help with a response plan. Some large healthcare organizations have gone so far as to purchase cyber-insurance to cover the losses incurred by a breach.

According to the Ponemon Institute's report, most healthcare organizations have an incident response process in place. Sixty-nine percent have a process with involvement from IT, information security, and compliance.

"As opposed to an organization trying to invest more money in firewalls or other types of technical solutions to protect against an intrusion, at this point you almost have to assume your network has already been breached," says Rick Kam, president of ID Experts, a data breach software and services provider. Looking at your internal systems and identifying where vulnerabilities lie, he says, will inform where you need to apply resources.

In the meantime, healthcare providers, as a class, are still struggling to deal with what is for them an elevated cyber-liability risk. Their low overall level of security, high value of PHI, and regulatory oversight makes any data breach a compliance nightmare waiting to happen. But as the mega breaches of 2014 and 2015 have amply shown, suffering a data breach in the healthcare sector is never a matter of if. It is a matter of when. ■

WORKING WITH EHR & HEALTH IT DEVELOPERS

Below is an excerpt from the Guide to Privacy and Security of Electronic Health Information issued by the Office of the National Coordinator for Health Information Technology.

When working with EHR and health IT developers, you may want to ask the following questions to help understand the privacy and security practices they put in place.*

- When my health IT developer installs its software for my practice, does its implementation process address the security features listed below for my practice environment?

  o Electronic protected health information encryption
  o auditing functions
  o backup and recovery routines
  o unique user IDs and strong passwords
  o role- or user-based access controls
  o auto time-out
  o emergency access
  o amendments and accounting of disclosures

- Will the health IT developer train my staff on the above features so my team can update and configure these features as needed?
- How much of my health IT developer's training covers privacy and security awareness, requirements, and functions?
- How does my backup and recovery system work?

  (1) Where is the documentation?
  (2) Where are the backups stored?
  (3) How often do I test this recovery system?

- When my staff is trying to communicate with the health IT developer's staff, how will each party authenticate its identity? For example, how will my staff know that an individual who contacts them is the health IT developer representative and not a hacker trying to pose as such?
- How much remote access will the health IT developer have to my system to provide support and other services? How will this remote access be secured?
- If I want to securely email with my patients, will this system enable me to do that as required by the Security Rule?

Source: The Office of the National Coordinator for Health Information Technology.

*For additional information about questions to ask health IT developers, see the Questions for EHR Developers document at http://bit.ly/EHRdevqs.