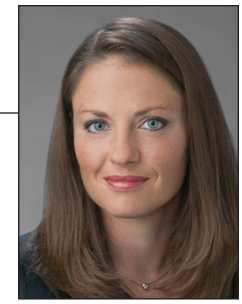

by Rachel V. Rose

Learning From the SEC

What Counsel Need To Know About Cybersecurity

Regardless of size, industry, and public or private status, all businesses need to be aware of cybersecurity initiatives. This need stems from various laws (i.e., the Health Insurance Portability and Accountability Act (HIPAA) and Gramm–Leach–Bliley Act (GLBA)),[1] cyberattacks, and breaches, which span across a multitude of industries ranging from retail to health care. The Target[2] and Community Health Systems (CHS)[3] breaches are two examples of public companies in different sectors that experienced significant data breaches and disclosed it on their Securities and Exchange Commission (SEC) filings.

The Target and CHS breaches raise several issues. Although breach disclosure requirements are inherent in many laws, such as HIPAA, public companies must also comply with the Securities Exchange Act of 1934's (Exchange Act) disclosure requirements.[4] Disclosure encompasses more than just SEC filings. It also extends to misrepresentations of compliance with the law. This article will address SEC laws and guidance, highlight the examples in relation to the SEC's guidance, and highlight ways to mitigate the risk of an attack.

SEC Items

Under the Exchange Act, companies are required to inform the public of "material corporate events."[5] In addition to the annual report (Form 10-K) and quarterly reports (Form 10-Q), "Form 8-K is the 'current report' companies must file with the SEC to announce major events that shareholders should know about."[6] A Form 8-K is what CHS and Target utilized to disclose the breach information to the public.

A common question that companies must address in relation to announcing a cybersecurity event is how much information to disclose. This is a balancing test of providing enough information to effectively disseminate the significance of the event to the public without providing too much information, which could further compromise the company. Thankfully, the SEC-issued guidance, which companies should use to set parameters of what to include in the Form 8-K, is on the Internet and in other forums. Specifically,

> We are mindful of potential concerns that detailed disclosures could compromise cybersecurity efforts—for example, by providing a "roadmap" for those who seek to infiltrate a registrant's network security—and we emphasize that disclosures of that nature are not required under the federal securities laws.[7]

As will be shown in the next section, CHS struck the perfect balance between the information it provided and meeting both its SEC and HIPAA requirements. Before moving on, another item to highlight is the misrepresentation of meeting cybersecurity standards and legal requirements. Recently, the SEC barred an advisory firm's president and owner from participating in the advisory and brokerage industry and fined him for "misrepresenting his firm's performance and its compliance with GIPS, the global investment performance standards."[8] Whether GIPS, HIPAA, or SOX (Sarbanes-Oxley Act) compliance, there are significant consequences for misrepresenting compliance. If a public company does this on its website or in an SEC filing, it could be grounds for a 10-b action. Under §240.10b-5,

> [i]t shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange,
> (a) To employ any device, scheme, or artifice to defraud,
> (b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or
> (c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security. [9]

This underscores the importance of being earnest in all company and financial institution statements.

Rachel V. Rose, J.D., MBA, is the chair of FBA's Corporate and Associations Counsel Division and co-author of What Are International HIPAA Considerations? *and* The ABCs of ACOs. *She can be reached at* rvrose@rvrose.com.

Actual Disclosure Highlights

As indicated above, the SEC's guidance underscores the importance of disclosure in relation to protecting the cybersecurity of the organization. CHS' Aug. 18, 2014, Form 8-K is an example of exactly what to do in the event this type of material disclosure is necessary. Item 8.01 contained the following statement:

> In July 2014, Community Health Systems, Inc. (the Company) confirmed that its computer network was the target of an external, criminal cyber attack that the Company believes occurred in April and June, 2014. The Company and its forensic expert, Mandiant (a FireEye Company), believe the attacker was an "Advanced Persistent Threat" group originating from China who used highly sophisticated malware and technology to attack the Company's systems. The attacker was able to bypass the Company's security measures and successfully copy and transfer certain data outside the Company. Since first learning of this attack, the Company has worked closely with federal law enforcement authorities in connection with their investigation and possible prosecution of those determined to be responsible for this attack. The Company also engaged Mandiant, who has conducted a thorough investigation of this incident and is advising the Company regarding remediation efforts. Immediately prior to the filing of this Report, the Company completed eradication of the malware from its systems and finalized the implementation of other remediation efforts that are designed to protect against future intrusions of this type. The Company has been informed by federal authorities and Mandiant that this intruder has typically sought valuable intellectual property, such as medical device and equipment development data. However, in this instance the data transferred was non-medical patient identification data related to the Company's physician practice operations and affected approximately 4.5 million individuals who, in the last five years, were referred for or received services from physicians affiliated with the Company. The Company has confirmed that this data did not include patient credit card, medical or clinical information; the data is, however, considered protected under HIPAA because it includes patient names, addresses, birthdates, telephone numbers and social security numbers. The Company is providing appropriate notification to affected patients and regulatory agencies as required by federal and state law. The Company will also be offering identity theft protection services to individuals affected by this attack. The Company carries cyber/privacy liability insurance to protect it against certain losses related to matters of this nature. While this matter may result in remediation expenses, regulatory inquiries, litigation and other liabilities, at this time, the Company does not believe this incident will have a material adverse effect on its business or financial results.[10]

This example stated the event, provided how the breach occurred, relayed the number of people who were impacted, referenced the relevant law, and indicated its action steps. By articulating the limited set of facts, CHS did not disclose any IT infrastructure issues that would make its system and, in turn, its patient and billing data, more vulnerable. In the event of a breach, this statement by CHS should be used as an example of what specificity of information should be disclosed.

Mitigation Techniques

An excellent starting point to mitigate the risk of a breach is to have the organization undergo a third-party risk assessment. Many public companies and some private companies utilize the SSAE 16 Auditing Standard. SSAE 16 is broken down into three main report types: SOC 1, SOC 2, and SOC 3. While SOC 1 addresses financial reporting controls, SOC 2 evaluates an entity's IT system in relation to the availability, confidentiality, and integrity of the data in three major control areas: technical, administrative, and physical. [11] "The SSAE 16 is an enhancement to the current standard for Reporting on Controls at a Service Organization, the SAS70."[12] While SAS70 reports are no longer utilized, some aspects of these reports translate to SSAE 16.

"Developed by the American Institute of Certified Accountants, The Statement on Auditing Standards No. 70 serve[d] as a widely recognized auditing standard for control activities and related processes over information technology. The SAS 70 Type II Standard periodically tests the effectiveness of internal controls. Laws such as the Investment Advisors Act of 1940 and Sarbanes-Oxley expressly prescribe its use.

"Unlike various securities laws, the standards set forth by HHS do not expressly indicate that an SAS 70 Type II audit is required, nor does it provide that this audit assures compliance with all the required elements of HIPAA and the HITECH Act. Furthermore, as the chart demonstrates, there is not a one-for-one match between the HHS Standards and SAS 70 Audit Control Objectives." (For SAS 70 and HIPAA Security Standards, *see* www.sas70.us.com/industries/hipaa-and-sas70.php.)

HHS Standards	SAS 70 Audit Control Objectives
Security Management Process	Five Elements of Internal Control
Information Access Management	Logical Security
Transmission Security	Network Security

"In the area of information technology, an SAS 70 Type II audit needs to clearly address the scope of the audit and the entity requesting the audit needs to communicate to the auditor all of the HIPAA and HITECH Act standards being evaluated. Therefore, if an entity promotes or stipulates in its contracts that it conducted a HIPAA/HITECH Act SAS 70 Type II audit, but did not address all of the Privacy, Security and Breach Notification Rule requirements, including evaluating business associate agreement compliance, this could amount to a material misrepresentation and detrimental reliance."[13] This initial assessment and subsequent annual assessments will provide companies with a starting point for assessing where the gaps are and what needs to be fixed.

Conclusion

Cybersecurity and disclosure requirements should not be taken lightly. The process is ongoing and should be incorporated into an organization's risk management or enterprise risk management program. Learning from other companies' experiences is crucial and can mitigate a similar event from occurring elsewhere. Continuing to monitor the SEC's website is a great place to start for guidance. ⊙

Corporate and Association Council Division continued on page 38

CORPORATE AND ASSOCIATION COUNCIL DIVISION continued from page 18

Endnotes

[1]*See* Pub. L. 104-191 (Aug. 21, 1996) and Pub. L. 106-102 (Nov. 12, 1999).

[2]Target Corp., *Form 8-K Filing* (Nov. 19, 2014), *available at* investors.target.com/phoenix.zhtml?c=65828&p=irolSECText&TEXT=aHR0cDovL2FwaS50ZW5rd2l6YXJkLmNvbS9maWxpbmcueG1sP2lwYWdlPTk5MTE0NTMmRFNFUT0yJlNFUT04JlNREVTQz1TRUNUSU9OX1BBR0UmZXhwPSZzdWJzaWQ9NTc%3D.

[3]Community Health Systems, *Form 8-K Filing* (Aug. 18, 2014), *available at* www.sec.gov/Archives/edgar/data/1108109/000119312514312504/d776541d8k.htm.

[4]Securities Exchange Act of 1934, Pub. L. 112-158 (Aug. 10, 2012).

[5]U.S. Securities and Exchange Commission, *Form 8-K*, available at www.sec.gov/answers/form8k.htm (last accessed June 5, 2015).

[6]*Ibid.*

[7]U.S. Securities and Exchange Commission, *SEC Guidance (*Oct. 13, 2011), *available at* www.sec.gov.

[8]*SEC Bars, Fines Advisory Owner for Misrepresenting GIPS Compliance*, blogs.reuters.com/financial-regulatory-forum/2014/06/03/sec-bars-fines-advisory-owner-for-misrepresenting-gips-compliance (last accessed June 5, 2015).

[9]13 FR 8183, Dec. 22, 1948, as amended at 16 FR 7928 (Aug. 11, 1951).

[10]*Supra*, n. 3.

[11]*See* www.ssae-16.com.

[12]*Ibid.*

[13]Rachel V. Rose, *HIPAA/HITECH Risk Assessments: Are the Standards Being Met?*, Becker's Hospital Review (Aug. 15, 2012), *available at* www.beckershospitalreview.com/healthcare-information-technology/hipaahitech-risk-assessments-are-the-standards-being-met.html.

IN THE LEGAL COMMUNITY: NORTH FLORIDA continued from page 34

tendees' concrete, specific suggestions for change related to mentoring, including the creation of a program to mentor and provide scholarships to at-risk minority high-school students, the provision of free or reduced-price memberships to local bar associations for young and government lawyers, and the development of a diversity mentoring event for minority law students, local lawyers, and judges.

Attorney wellness was another focus during the panel and table discussions. During the judicial panelist discussion, Judge Scriven urged lawyers to take care of themselves and their physical health, to commit to jobs they love and know that the wealth will follow. She also advised the women lawyers in the room to invest in a good pair of flats to promote their happiness, as well as encouraged lawyers to never say yes right away when someone asks them to commit to something (unless it's the president, of course—then they should say yes!).

Judges and attorneys present at the event were also interested in balancing a demanding career with their family commitments. In fact, many of the participants suggested that family-friendly workplace and bar association policies were critical to happiness and diversity. They suggested hosting family-friendly bar meetings and socials, limiting work demands during family times, allowing attorneys more flexibility by working remotely, creating more generous maternity- and paternity-leave policies, and developing child-friendly spaces in offices and courthouses.

Finally, the panelists and small groups discussed happiness for minorities and diverse communities within the legal profession. Women and people of color are entering the legal profession at higher rates than ever before, yet too few seem to stay. To this end, participants emphasized the importance of giving young minority lawyers client control on legal matters, thus increasing their professional autonomy, and continuing work on bridging the female leadership gap in the legal profession by appointing more women to leadership positions in law firms.

However individualized the definitions of happiness and success might be, the 2015 Leadership Roundtable discussion demonstrated that most lawyers are not that different. As a group, we want to feel like our decisions matter, that our opinions have been heard, and that we have support from those closest to us—an experience created and shared during the roundtable itself. ⊙

IN THE LEGAL COMMUNITY: 50TH ANNIVERSARY continued from page 37

We continue to work together as respected colleagues.

More than any court I know of, our judges work together as friends and colleagues.

I hope you will excuse a brief personal reference. In this neighborhood, I worked on the docks, in the freight yards, and in an office for a small trucking firm while going to free Brooklyn College at night. Aspiring to be a federal judge would have been absurd. I argued my first motion before this court in a Post Office courtroom across the street more than 60 years ago. Almost half a century ago, when a half dozen judges did its work, I joined it, turning to them for guidance. Chief Judge Joseph Zavatt, Judge Jacob Mishler, and Judge John Dooling set the court's tone of practicality and compassion that still marks our work.

Over the years, our judges and magistrate judges, despite a huge increase in number, have continued to share a deep affection—and an unwavering desire to provide the rule of law to all our people in this district.

New York's senators and our presidents have ensured the high quality of our bench—women and men, representative of our district's ethnic diversity, many of us lifted to this high office from humble beginnings.

The decisions of our individual trial judges, our magistrate judges, and our bankruptcy judges depend in important part on each of our diverse backgrounds. The luck of the draw is a necessary aspect of judicial independence.

Each of us respects each judge's view of the judge's role. For example, a number of our judges and magistrate judges work closely with pretrial and probation services and outside agencies in criminal diversion and treatment programs that are admired throughout the nation. Other judges take a more traditional view.

We know our community. We have been around the block.

What a joyful and humbling experience it has been for each of us to participate in the work of this great court. Paraphrasing the poet Elizabeth Barrett Browning, "We love this court with the breath, smiles, tears of all our lives! and … we shall love it and the law ever better in the years ahead." ⊙