Health Lawyers Weekly

August 08, 2014 Vol. XII Issue 30

Cybersecurity and the Health Care Board

By Michael W. Peregrine and Edward G. Zacharias, McDermott Will & Emery LLP

A series of recent developments serve to encourage health care boards to more formally embrace oversight responsibility for cybersecurity and data protection matters. These developments include prominent examples of data breaches; high-level governmental emphasis on board cybersecurity focus; regulatory enforcement of privacy statute violations; private party litigation; and important new surveys and "whitepapers" from influential governance policy organizations.[1] Collectively, they reflect an increasing focus on the board's cybersecurity role. It is a role that is particularly relevant to the health care sector, with its unique relationship to patient privacy and data security.

This is not a question of "jumping on the bandwagon" or following the latest governance "fad." Nor is it entirely a question of breach remediation and mitigation tactics, which are reactionary measures. Rather, it is a clear evolution of governance standards as they relate to data protection and cybersecurity. The organizational focus is noticeably moving "from the IT department to the boardroom."[2]

Some of these developments are general in nature and apply across industry sectors. Others apply very specifically to the health care sector. Together, they reflect a growing consensus on the related oversight expectations of corporate governance.

General Developments

The respected National Association of Corporate Directors (NACD)strongly endorses a clear board cybersecurity oversight role. In "Cyber-Risk Oversight," the latest edition of its "Directors' Handbook Series," NACD sets forth five key principles for corporate board consideration:

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber risk management should be given regular and adequate time on the board meeting agenda.

4. Directors should set the expectation that management will establish an enterprise-wide cyber risk management framework with adequate staffing and budget.

5. Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.[3]

The Securities and Exchange Commission (SEC) is similarly supporting board awareness of cyber risk. In a June 10 speech, SEC Commissioner Luis Aguilar encouraged boards to include cyber preparedness as an important element of their risk oversight duties.[4] Noting the many known risks to corporations arising from cyber-threats, Commissioner Aguilar expressed concern that a gap may exist between the magnitude of these risks and the level of board preparedness.[5] Boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility do so at their own peril.[6]

Also notable are efforts by the Federal Trade Commission (FTC) to require companies across industry sectors to implement policies and procedures designed to protect personal data.[7] The FTC's position is reflected in enforcement action (e.g., the recent Snapchat settlement) and not based on any particular statute or regulation.[8] The essence of the FTC position is that companies should develop a comprehensive written information security program under the direction of a designated employee, that is reasonable and designed to be responsive to the information security needs of its business operations.[9] The FTC Chair has also asked Congress for regulatory authority to more specifically deal with cyber risk issues.[10]

Also worth noting is the series of recent, highly publicized data thefts suffered within the last year by several major US corporations (see, e.g., recent "hacking" of The Wall Street Journal).[11] The companies suffering these thefts have been subjected, in varying degrees, to reputational damage, internal investigation costs, legal and consultant fees, compensation to aggrieved consumers, litigation (e.g., class actions), regulatory scrutiny, and significant constituent efforts to hold executives and the board directly and personally accountable for such damage.[12] Indeed, recent developments demonstrate

how data breaches arising from cyber attacks can expose directors to shareholder derivative and similar actions asserting breach of fiduciary duty (i.e., that the board failed to assure implementation of adequate information security measures).[13]

In addition, concerns are also arising with respect to "cloud-based" cybersecurity as a subset of more global cybersecurity issues. Knowledgeable observers are recommending that boards have a working knowledge of the risks associated with cloud-focused data storage mechanisms, and with cloud-based service providers.[14]

Health Care Developments

More relevant, from a health care governance perspective, is the series of compelling recent cyber risk developments affecting the health care sector.

For example, the Department of Health and Human Services, Office for Civil Rights (OCR) has been vocal about Health Insurance Portability and Accountability Act (HIPAA) enforcement being an agency priority.[15] The agency's increased attention to enforcement is likely due to a variety of factors, including its volume of active investigations prompted by the ever-increasing pipeline of HIPAA complaints and reported breaches[16], Congressional pressure to meet its statutory enforcement mandate[17], and a recent Office of Inspector General investigation criticizing OCR's enforcement practices.[18] In a press release announcing a 2013 breach settlement with Shasta Regional Medical Center in California, former OCR Director Leon Rodriquez stated: "[s]enior leadership helps define the culture of an organization and is responsible for knowing and complying with the HIPAA privacy and security requirements to ensure patients' rights are fully protected."[19] While there has recently been a notable amount of turnover in top-level HIPAA staff at OCR, there is nothing to suggest that the new leadership will refrain from making enforcement an ongoing priority.

The focus on enforcement has also been evidenced by annual upticks in the volume of complaints that OCR has resolved with corrective action. For example, 3,470 of the 4,463 complaints that OCR investigated in 2013 resulted in some form of corrective action.[20] Notably, just under half of all published HIPAA settlements between a covered entity and OCR that included a significant financial payment have occurred in the last year and a half.[21] In May, New York Presbyterian Hospital and Columbia University agreed to pay a combined $4.8 million to settle alleged HIPAA violations. The payment constituted "the largest HIPAA settlement to date."[22] In announcing the settlement, the Acting Deputy Director of Health Information Privacy at OCR stated that the case "should remind health care organizations of the need to make data security central to how they manage their information systems."[23] This fall, OCR will begin a second round of HIPAA

compliance audits of covered entities and business associates. Health care boards should take appropriate steps to ensure their organization is prepared for a potential audit.[24]

As noted above, the FTC has asserted its power to regulate unfair and deceptive practices under Section 5 of the FTC Act in pursuing data security actions against companies. In doing so, the agency has periodically targeted health care companies for insufficient cybersecurity practices. In some cases, these actions have been coordinated with OCR,[25] but the FTC has also independently pursued enforcement actions against health care companies. Unlike OCR, which, to date, has only pursued HIPAA covered entities, the FTC has also filed actions against business associates. In January, a company that provides medical transcription services to covered entities settled FTC allegations that it violated the FTC Act when it hired subcontractors whose "inadequate security" practices resulted in the unauthorized disclosure of medical transcript files.[26] While there remains vigorous debate about the FTC's jurisdiction to regulate data security practices under its Section 5 authority,[27] the agency continues to aggressively pursue enforcement actions. Accordingly, health care boards should ensure their cybersecurity programs are sufficient in light of FTC precedent.

Health care companies have also found themselves "in the crosshairs" of state Attorneys General, who now have authority to enforce HIPAA[28] in addition to their traditional jurisdiction over state consumer protection laws and regulations. While most state Attorneys General have been slow to embrace their relatively-new HIPAA enforcement authority, these actions will likely increase as state regulators become more comfortable with HIPAA. Moreover, a number of state Attorneys General are actively enforcing their state's data breach notification laws against health care companies.[29] In a recent, notable case, a state whose residents were affected by a breach at a hospital located in a neighboring state sought to enforce its data breach law against that hospital. Last month, the hospital agreed to pay $150,000 to settle the allegations.[30]

In addition to enforcement actions by regulators, a number of lawsuits have also been filed by individual consumers or classes of consumers in response to security breaches. Even where the applicable cybersecurity laws and regulations do not provide for a private right of action, plaintiffs have stated claims for negligence, invasion of privacy, breach of contract, misappropriation of confidential financial information, unjust enrichment, breach of fiduciary duty, fraud, identity theft, and violation of consumer protection statutes. Courts are increasingly granting defendants' motions to dismiss such claims, particularly in light of the U.S. Supreme Court's ruling in *Clapper v. Amnesty International, USA*[31] where the Supreme Court found that Article III standing requires imminent harm that is tied to the litigated action. Accordingly, courts are consistently denying claims for injuries based on potential harm where plaintiffs have failed to demonstrate actual damages or breaches of confidentiality.

For example, lawsuits against a large academic medical center in the Mid-West[32] and a California health system have recently been dismissed on such grounds. However, plaintiffs pursuing similar claims that do not arise under federal law may not be doomed by the *Clapper* decision. In other circumstances, health care organizations have settled these claims for substantial amounts in order to avoid potentially more costly litigation. For example, Stanford Hospital and two of its business associates recently agreed to pay $4.1 million to settle a class action lawsuit arising from a breach that resulted in the medical information of approximately 20,000 emergency room patients being made publicly available on the internet for a period of nearly a year.[33]

Regardless of the jurisdiction, these cases speak clearly to the organizational risks associated with data breaches by, or otherwise involving, a health care company. They also suggest the enormous costs associated with responding to breaches, and serve as a strong reminder why health care boards should focus on implementing cybersecurity practices that are aimed at preventing a data breach.

Board Action

There is no “one size fits all”/recognized “best practice” governance approach for the health care board to adopt in response to these developments. The board will need to craft its approach in a manner that best suits the organization’s unique circumstances. As many health care boards have encountered with quality of care matters, this can often prove a daunting task when the focus of the oversight responsibility is something complex, technical, or otherwise foreign to the typical board member’s skill set. The NACD’s “Handbook” will be a helpful guide to board efforts to more fully understand their oversight role regarding cyber risks.

So, the first step towards this goal may be to assure board “buy-in” to the issue; to support its “embrace” of cybersecurity as a governance oversight responsibility and not as the exclusive province of the CIO and his/her team.

The next step is to provide the board with a fundamental awareness of cyber issues as they present to the organization. This has an external component -- a briefing on applicable laws and recent risk related development. It also has an internal component -- reviewing with the board the depth of the organization’s IT staff; existing cyber-based policies and procedures; prior organizational history with cyber issues; and how cyber issues have previously been presented to the board.

The third step is to determine the most appropriate forum for enhanced cyber oversight; a new standing committee, a current standing committee (e.g., Audit or Compliance), or the board as a whole (as many boards choose to address their enterprise risk

management oversight responsibilities). It may also identify the extent to which intra-leadership (e.g., Committee to Committee, executive to executive) coordination is necessary. In this regard, it is important that the compliance officer and the general counsel be closely involved in the establishment of oversight protections. Many of the private litigation and regulatory enforcement actions against officers and directors are based on *Caremark*-based risk oversight themes; i.e. that the data breach or similar cyber event was a direct result of the board's failure to implement and monitor an effective internal cyber risk management system.

A fourth step is to incorporate the need for candidates with cyber-based background into the director nomination process. This is clearly consistent with the movement towards a competency based board; cyber oversight is more likely to succeed with the presence of at least one subject matter expert on the board (or responsible committee).

A fifth step is to work with the organization's general counsel to determine the extent to which existing indemnification and officer's and director's insurance policies provide protection to data breach-based legal actions asserting personal liability against board members.

A sixth and final beginning step is to achieve an understanding with the CEO and CIO on what matters are properly reserved to the CIO, what matters require board awareness, and what matters require board/committee oversight, action, and/or approval. (If the organization also has a chief privacy officer, that person should also be included within this discussion). This would include an agreement on upstream risk reporting, and on what level of continuing board/committee education on cyber matters is necessary to support effective oversight. In this regard, the board should be aware of, and respond to, a new survey that suggests that health care CIOs often bear a disproportionately high degree of responsibility for organizational data breaches.[34] The nature of cyber risk is such that all executive level employees should be encouraged by the board to support the CIO and the board in the implementation and operation of effective data security programs.

There is overwhelming evidence suggesting that health care boards must adopt a more organized and concerted approach to matters of cybersecurity and data protection. Such an approach can be assisted by valuable guidelines prepared by organizations such as NACD, and should reflect a full awareness of current developments in the area. The general counsel, compliance officer, and the CIO can be valuable participants with the CEO in supporting board efforts to embrace more vigorous awareness of, and attention to, cyber risks.

[1] *See*, *generally*, Kirk J. Nahra, "Privacy and Data Security Is For Everyone: Common Matters That All Companies Should Address," Bloomberg BNA Corporate Law & Accountability Reporter, July 18, 2014; Peter J. Isajiw and John C. Vasquez, "Cybersecurity Risks Reviewed: Directors and Officers Must Be Proactive and Prepared," Bloomberg BNA Corporate Law & Accountability Reporter, July 22, 2014.

[2] Brad Walz, "Cybersecurity: Having a Privacy a Policy is Not Enough," JD Supra Business Advisor, July 2. 2014; *see also* Danny Yadron, "Boards Race to Fortify Cybersecurity," The Wall Street Journal, June 29, 2014.

[3] National Association of Corporate Directors, Director's Handbook Series 2014, "Cyber Risk Oversight," at p. 4.

[4] Luis A. Aguilar, Commissioner, U.S. Securities and Exchange Commission, "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus."

[5] *Id.*

[6] *Id.*

[7] Nahra, *supra* note 1.

[8] *Id.*

[9] *Id.*

[10] Isajiw and Vazquez, *supra* note 1, citing *Prepared Statement of The Federal Trade Commission on Protecting Personal Consumer Information from Cyber Attacks and Data Breaches*, testimony before Senate Committee on Commerce, Science, and Transportation (March 26, 2014).

[11] http://online.wsj.com/articles/wsj-takes-some-computer-systems-offline-after-cyber-intrusion-1406074055.

[12] Isajiw and Vazquez, *supra* note 1; Nahra, *supra* note 1.

[13] David L. Barres and Dominic J. Picca, "Determining Director Liability for Cybersecurity Risks," CorporateCounsel.com, August 6, 2014, in which the authors reference a recent derivative action filed by a shareholder of a major international hotel/residential lodging company following the theft of over 600,000 consumer payment card data.

[14] Paul A. Ferrillo, "Cloud Cyber Security: What Every Director Needs to Know," The Harvard Law School Forum on Corporate Governance and Financial Regulation, August 6, 2014.

[15] *See e.g.*, Jeff Overley "Big Year Ahead For HIPAA Fines, HHS Atty Says," Law360 (June 12, 2014).

[16] *See* OCR's *Annual Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Years 2011 and 2012* (last accessed August 5, 2014); OCR Enforcement Numbers at a Glance (last accessed August 5, 2014).

[17] *See Your Health and Your Privacy: Protecting Health Information in a Digital World*: Hearing Before the Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary, 112th Congress (November 9, 2011).

[18] *See* Office of the Inspector General Report, *The Office for Civil Rights Did Not Meet All Federal Requirements in its Oversight and Enforcement of the Health Insurance Portability and Accountability Act Security Rule* (November, 2013).

[19] *See* HHS Press Office, "HHS Requires California Medical Center to Protect Patients' Right to Privacy" (June 13, 2013).

[20] *Id.; see also supra* note 16, OCR Enforcement Numbers at a Glance.

[21] Published HIPAA settlements involving a significant financial component by year: 2014 (6 as of August 6, 2014); 2013 (4); 2012 (5); 2011 (2); 2010 (2); 2009 (1); and 2008 (1).

[22] *See* HHS Press Office, "Data Breach Results in $4.8 million HIPAA Settlements" (May 7, 2014).

[23] *Id.*

[24] *See* D. Gottlieb, E. Zacharias & P. Callaghan, "OCR to Begin Phase 2 of HIPAA Audit Program" (July 29, 2014), *available at:* http://www.mwe.com/OCR-to-Begin-Phase-2-of-HIPAA-Audit-Program-07-29-2014/.

[25] *See e.g.*, OCR Press Office, "Rite Aid Agrees to Pay $1 Million to Settle HIPAA Privacy Case" (last visited August 6, 2014); FTC Press Office, "Rite Aid Settles FTC Charges That It Failed to Protect Medical and Financial Privacy of Customers and Employees" (last visited August 6, 2014).

[26] FTC Press Office, "Provider of Medical Transcript Services Settles FTC Charges that it Failed to Adequately Protect Consumers' Personal Information" (January 31, 2014).

[27] *See e.g.,* In the Matter of LabMD, Inc.

[28] 42 U.S.C. 1320d–5(d).

[29] Note that a data breach caused by a health system's outside revenue cycle vendor served as the basis for an extensive and highly public business practices investigation of the health system in 2012 by the state attorney general. As part of its settlement of litigation filed by the attorney general, the revenue cycle vendor accepted a six year ban on doing business in the state.

[30] Martha Kessler, "Massachusetts Enforces Across Border As R.I. Hospital Settles Breach Notice Case" Bloomberg BNA (July 28, 2014).

[31] 133 S. Ct. 1138 (2013).

[32] *See e.g.,* Joseph Conn, "Advocate Beats Second Class-Action Suit, Faces Others Over 2013 Data Breach," Modern Healthcare (July 14, 2014).

[33] Jason Greene, "$4.1M Settlement Possible in Stanford Medical Information Breach," San Jose Mercury News (March 22, 2014).

[34] Joyce E. Cutler, "Chief Information Security Officers Viewed as Scapegoats in C-Suite Survey," BloombergBNA Corporate Law & Accountability Report, August 6, 2014.

1620 Eye Street NW
Washington, DC 20006-4010
Phone: 202-833-1100 Fax: 202-833-1105