Nassau Lawyer

JUNE 2016 | VOL. 65 | NO. 10 | WWW.NASSAUBAR.ORG

Addressing a Health Care Organization's Cyber Risks Begins at the Top

On March 28, 2016, hackers crippled the systems of MedStar Hospitals with an alleged ransomware attack and forced MedStar to shut down the computers, network, and email for its ten hospitals and 250 outpatient centers and resort to pen and paper.[1] Hospitals, health insurance companies, medical providers and other health care related organizations (collectively "Health Care Organizations") continue to be targeted by hackers and cyber criminals for the treasure trove of information stored on their respective medical and corporate systems. The target-rich environment includes protected health information (PHI) and personally identifiable information (PII) which can be used for tax fraud, credit card fraud, extortion, and prescription fraud, to name a few profitable schemes. The challenges associated with protecting this information are enough to keep board members and executives (collectively "Senior Management") awake at night.

John J. Cooney

The rapid increase in the frequency of data breaches has also spawned a new regular occurrence — lawsuits and regulatory investigations targeting Senior Management and their actions, or lack thereof. In other words, gone are the days in which managing cybersecurity risks was solely the responsibility of a Heath Care Organization's chief information officer and/or its information technology department ("IT"). Given the context of today's cyber world, Senior Management must make data breach prevention and detection part of their Health Care Organization's overall risk management framework.

Managing cyber risks will most likely be new and unlike many other aspects of risk management for many in Senior Management. Indeed, it might be outright intimidating given the particular technical disciplines. With that said, however, Senior Management needs to ensure that they are able to understand the different issues and ask the right questions to become informed. For some guidance on where Senior Management should start, let us consider a couple of lawsuits, including the current action involving Anthem Blue Cross Blue Shield ("Anthem"). On February 5, 2015, Anthem announced that a data breach had occurred involving approximately 80 million records. Less than twelve hours later, the first of more than 100 lawsuits was filed. The cases have now been consolidated into a multidistrict litigation proceeding in the United States District Court, Northern District of California.[2]

In the consolidated amended class complaint, plaintiffs allege, inter alia, negligence, negligence per se, negligent misrepresentation, breach of the implied covenant of good faith and fair dealing, breach of contract and unjust enrichment. It is alleged that Anthem "failed to take even the most basic security precautions," such as changing passwords, to protect PII (e.g. Social Security numbers, birthdates and billing information) and hackers took advantage of Anthem's "grossly inadequate computer systems and data security practices." Moreover, Anthem is alleged to have breached their obligation to notify affected individuals and regulators in a timely manner. Whether it is Anthem or other high profile breaches and the resultant lawsuit (e.g. Target, Home Depot), allegations and regulatory scrutiny generally involve a failure to assess an organization's vulnerabilities and update systems, failure to implement reasonable data security policies, deploy resources appropriately, detect breaches, and respond to any incidents in a meaningful, timely way. In other words, there are simple and basic steps that Senior Management can take to immediately mitigate liability associated with a cybersecurity incident.

Assess Vulnerabilities and Periodically Review

As an initial step, an existing member of Senior Management should be designated as the cybersecurity lead to focus on data security matters. If that individual does not exist, Senior Management should take steps to form a cybersecurity risk committee of internal and external experts. In other words, Senior Management is not expected to be experts in cybersecurity, but they are held responsible for overseeing the risk and ensuring that resources are dedicated to addressing it. At a minimum, a cybersecurity risk committee should be tasked with regularly briefing Senior Management on its assessment of the Health Care Organization's vulnerabilities and progress to implement security enhancements and policies, detect breaches, train resources, and any gaps with regard to federal or state law.

Besides the above-referenced allegations in the *Anthem* matter, the need for Senior Management to be actively involved in managing a Health Care Organization's cyber risks is illustrated in the opinion dismissing the shareholder derivative suit filed against Wyndham Worldwide Corporation's directors and officers.[3] In that suit, plaintiffs alleged that Wyndham suffered injury because of three data breaches, and that the failure to adequately oversee the company's cybersecurity and implement reasonable security measures allowed hackers to steal customer's card account information. The district court dismissed the suit and noted that the board and its audit committee discussed the data breaches, Wyndham's security policies and potential enhancements at fourteen meetings over nearly four years, and "[t]he Audit Committee reviewed the same matters in at least

sixteen meetings" during the same period of time.[4] Moreover, the court explained that Wyndham hired external experts to investigate, assess and make recommendations with regard to each breach and Wyndham began to implement the recommendations.[5] In sum, the engagement by Senior Management in managing cybersecurity risks can significantly reduce, if not eliminate, liability. Indeed, as *Wyndham* highlights, even where Senior Management could not prevent multiple breaches from occurring, the direct and proactive involvement by Senior Management can be dispositive.

Implement and Test a Breach Incident Response Plan

Senior Management should also ensure that their Health Care Organization has prepared and tested a breach incident response plan for any cyber incident. As referenced above, the trove of information available to cyber criminals includes PHI as well as PII. Thus, Senior Management needs to be aware of state breach notification requirements in addition to the Health Care Organization's obligations under HIPAA.[6] In short, if a breach involves PII (e.g. Social Security numbers), a Health Care Organization must wade through their patients' residency and then analyze the patchwork of state laws (forty-seven states and the District of Columbia have passed laws requiring notification) to determine the circumstances that require breach notification to patients and regulators.[7] By testing the breach incident response plan, Senior Management can ensure that the plan is ready for instant execution before a cyber incident occurs and, thus, mitigate the chances for further harm or scrutiny that the Health Care Organization did not notify affected individuals and regulators in a timely, accurate and meaningful manner.

As the court noted in *Wyndham*, the dismissal was based in part on the fact that the company hired external experts to investigate the breaches and make recommendations to enhance data security. There is, however, another reason for Senior Management to consider the engagement of external resources as part of its breach incident response plan. Until there is an explicit privilege for cybersecurity investigations and communications, a Health Care Organization needs to operate under the assumption that a cybersecurity investigation, which includes identifying vulnerabilities (and possibly an organization's negligence in not addressing them) is discoverable in a private suit or regulatory action. In other words, as part of its breach incident response plan, a Health Care Organization should have an external incident response team, including an attorney that it will utilize at the outset of any data breach investigation and subsequent stages to engage the services of a forensic technology team. A few months ago, the importance of this point was proven. The United States District Court for the District of Minnesota rejected plaintiffs' claims that Target improperly asserted attorney-client privilege and work-product claims over documents created by its outside counsel and Target's Data Breach Task Force.[8] The court shielded the majority of information sought by plaintiffs and found that outside counsel was retained to direct Target's forensic investigation, provide legal advice about the breach, and prepare to defend Target in litigation. In short, Senior Management should ensure that the breach incident response plan is carefully structured to include outside counsel and technical experts and that they are part of the testing to ensure that all aspects of a breach investigation are protected to the extent possible.

Conclusion

The rapid increase in private actions and increased scrutiny by regulators means that Senior Management should immediately understand and approach cyber risks like other major risks to a Health Care Organization and manage them accordingly, including frequent briefings of risks and threats and periodic evaluations of the organization's cyber risk profile. Senior Management's involvement cannot be overstated and proactive engagement can help transform sleepless nights into restful ones.

John J. Cooney, Esq. is a partner at Ruskin Moscou Faltischek and chair of the Firm's Cybersecurity and Data Privacy practice group. He is also a member of the Firm's Health Law Department and the White Collar Crime and Investigations practice group. Prior to becoming an attorney, Mr. Cooney was trained as a software engineer and had over a decade of experience analyzing and developing technology solutions for Fortune 500 companies. He can be reached via e-mail at jcooney@rmfpc.com.

1. *Virus infects MedStar Health system's computers, forcing an online shutdown*, Mar. 28, 2016, https://www.washingtonpost.com/local/virus-infects-medstar-health-systems-computers-hospital-officials-say/2016/03/28/480f7d66-f515-11e5-a3ce-f06b5ba21f33_story.html
2. *In Re Anthem, Inc. Data Breach Litigation*, Case No. 15-md.02617-LHK (N.D. Cal.)
3. See *Palkon v. Holmes*, No. 2:14-CV-01234 (SRC), *2014 BL 293380* (D.N.J. Oct. 20, 2014).
4. *Id.* at *3-4.
5. *Id.* at *4.
6. 45 CFR §§ 164.400-414
7. A Health Care Organization based in New York has to be concerned with HIPAA as well as the New York State Information Security Breach and Notification Act, which is comprised of section 208 of the State Technology Law and section 899-aa of the General Business Law.
8. *In re: Target Corporation Customer Data Security Breach Litigation*, MDL No. 14-2522 (Oct. 23, 2015).