MARCH 2023

Governance Feature

THE GOVERNANCE INSTITUTE

A SERVICE OF nrc HEALTH

Cyber Legal Cases and Trends Your Board Needs to Watch

By **Bob Chaput**, **Andrew Mahler**, and **Omenka Nwachukwu**, *Clearwater*

It is never a good idea for a company's board of directors to skip training on cybersecurity risk management oversight. There are two critical trends related to enterprise cyber risk management (ECRM) in healthcare that boards and senior executives should be aware of:[1]

1. The emergence of a de facto "standard of care" related to cyber risk management
2. The increasing possibility that legislatures, regulators, and the courts will hold executives and directors responsible for ECRM failures

This article highlights several foundational and recent cyber legal cases that healthcare boards should be mindful of. These cases may represent a trend towards expectations for greater board accountability for cyber risk management oversight.

All boards have fiduciary responsibilities. A *fiduciary* is a person or business with "the power and obligation to act for another (often called the beneficiary) under circumstances that require total trust, good faith, and honesty."[2] While the legal duties of directors are covered by federal securities laws as well, fiduciary duties are spelled out in state corporation laws, usually based on the American Bar Association Model for Business Corporation Act.[3]

Several of the cases discussed in this article are derivative lawsuits brought by shareholders of public companies who argued, some successfully, that specific boards did not execute their fiduciary duties when providing oversight of cyber risk management. It is important to note that all board directors in private, not-for-profit as well as public companies have legal fiduciary duties.

1 Bob Chaput, *Stop the Cyber Bleeding: What Healthcare Executives and Board Members Must Know About Enterprise Cyber Risk Management (ECRM),* Clearwater, 2020; Bob Chaput and Iliana Peters, "The Legal Liabilities of Enterprise Cyber Risk Management," American Health Law Association, February 1, 2021.
2 "Fiduciary," *The People's Law Dictionary*, 2002.
3 American Bar Association, *Model Business Corporation Act Annotated*, *Fifth Edition*, 2020.

It may be in these cyber-driven derivative and other suits where the word "risk" becomes a serious four-letter word for directors.

The Board and Risk Management Responsibilities

One of a board's top three critical responsibilities is providing risk oversight[4] (along with strategy planning oversight and executive leadership development).

In *Governance, Risk Management, and Compliance*, Richard Steinberg cites Jim Kristie, Editor and Associate Publisher of *Directors & Boards*, saying, "Frankly, boards have let down the nation and its capital markets. Boards have not had the right leaders in place; **they have not adequately analyzed risk**; they have not had the depth of knowledge of their company's operations that they should have had; they have not done a sufficient job of helping management see the big picture in front of them and in seeing around corners as to what lies ahead; and they have not acted smartly and speedily as conditions deteriorated and management faltered."[5]

So, where have board members let down investors regarding cyber risks and how have they failed to adequately analyze **cyber** risks? Let's examine some cases.

Cyber Legal Cases

One of a board member's fiduciary responsibilities is the duty of care: "a requirement that a person acts toward others and the public with the watchfulness, attention, caution, and prudence that a reasonable person in the circumstances would use."[6] If a person's actions do not meet this standard of care, the acts may be considered negligent and any damages resulting may be claimed in a lawsuit for negligence. For executives and board members, these fiduciary responsibilities demand paying much more attention to their organization's cyber risk management program.

Recent data-breach litigation shows how corporate executives and board members can be at risk of personal liability when a cybersecurity incident occurs. For example, in 2013, cyber attackers infiltrated retailer Target and gained access to the company's computer network via credentials stolen from a third-party vendor. The attackers

4 Martin Lipton, et al., "Risk Management and the Board of Directors," Harvard Law School Forum on Corporate Governance, March 20, 2018.
5 Richard M. Steinberg, *Governance, Risk Management, and Compliance*, John Wiley & Sons: Hoboken, New Jersey, 2011.
6 "Duty of Care," *The People's Law Dictionary*, 2002.

installed malware and accessed 41 million customer payment card accounts.[7] As a result of this breach:

[L]itigation was filed, regulatory and congressional investigations commenced, and heads rolled. Banks, shareholders, and customers all filed lawsuits against the company. Target's CEO was shown the door. And Target's directors and officers were caught in the crossfire. In a series of derivative lawsuits, shareholders claimed that the retailer's board and C-suite violated their fiduciary duties by not providing proper oversight for the company's information security program, not making prompt and accurate public disclosures about the breach, and ignoring red flags that Target's IT systems were vulnerable to attack.[8]

In Target's case, the shareholder derivative lawsuits filed against the company's officers and directors were dismissed. However, the severity of the case underscores "the critical oversight function played by corporate directors when it comes to keeping an organization's cyber defenses up to par."[9]

Derivative litigation was also brought against Yahoo, Inc., for data breaches that occurred in 2014 and 2016. The $29 million settlement, approved in January 2019, "represents the first significant recovery in a data-breach-related derivative lawsuit targeting directors and officers for breach of fiduciary duty."[10] In an article reviewing the implications of the Yahoo case, attorney Freya K. Bowen of law firm Perkins Coie said, "[A] series of prominent and widely publicized data breaches, combined with the growth of a cybersecurity industry designed to assist corporations in protecting against cyber-attacks, may have created a corporate cybersecurity standard of care… In other words, the very development of stronger cybersecurity protections and controls may have created a known duty to act. The Yahoo data breach derivative litigation could be a harbinger of this trend. Many of the suit's allegations assert a bad-faith failure by the directors to adequately monitor the corporation's cybersecurity system, including through their failure to adequately fund the corporation's data-security infrastructure and through their refusal to approve necessary security updates."[11]

7 Kevin McCoy, "Target to Pay $18.5M for 2013 Data Breach that Affected 41 Million Consumers," *USA Today*, May 23, 2017.
8 Craig Newman, "Lessons from the War Over the Target Data Breach," NACD BoardTalk, July 27, 2016.
9 *Ibid.*
10 Freya K. Bowen, "Recent Developments in Yahoo and Equifax Data Breach Litigation," Perkins Coie Tech Risk Report, February 6, 2019.
11 *Ibid.*

The 2017 Equifax Inc. data breach, which impacted 147 million consumers, was settled in July 2019 at a cost of at least $575 million and potentially up to $700 million.[12] The lawsuits that followed the Equifax data breach also named certain officers and directors of the organization:[13]

Although the court granted the motion to dismiss with respect to most of the officers and directors, it denied it as to the Equifax's former CEO, who was alleged to have personal knowledge of the inadequacies in Equifax's cybersecurity system. This ruling makes Equifax the first major data-breach related claim against a corporate officer to survive a motion to dismiss. These cases, along with the increase in cybersecurity-related derivative and securities actions, indicate that directors and officers of major corporations may face an increased risk of personal liability in connection with data breaches.[14]

> If a person's actions do not meet the duty of care standard, the acts may be considered negligent and any damages resulting may be claimed in a lawsuit for negligence. For executives and board members, these fiduciary responsibilities demand paying much more attention to their organization's cyber risk management program.

The Caremark Standard and Recent Cyber Cases

In 1996, the Delaware Court of Chancery issued its seminal decision in *In re Caremark International Inc. Derivative Litigation*, establishing the conditions for director oversight liability under Delaware law.[15] The board was sued by shareholders for breach of duty of care for allegedly failing to provide appropriate oversight of employee conduct, exposing the company to civil and criminal penalties. However, the board prevailed, and the court concluded that the board reasonably believed the

12 Federal Trade Commission, "Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach" (press release), July 22, 2019.
13 Bowen, 2019.
14 Bowen, 2019.
15 Edward B. Micheletti and Ryan M. Lindsay, "The Risk of Overlooking Oversight: Recent Caremark Decisions from the Court of Chancery Indicate Closer Judicial Scrutiny and Potential Increased Traction for Oversight Claims," Skadden, Arps, Slate, Meagher & Flom LLP, December 15, 2021.

practices were lawful and attempted in good faith to exercise employee oversight and monitoring responsibilities.

The case established the so-called "Caremark standard," which imposes liability under the following two circumstances: where "a) directors utterly failed to implement any reporting or information system or controls, or b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."[16]

A 2019 article examining *Marchand v. Barnhill*,[17] a subsequent case that affirmed and strengthened Caremark, stated, regarding derivative lawsuits, "Although Caremark claims will remain 'the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment,' we expect an increase in attempted derivative litigation over a purported lack of board-level monitoring systems for specific risks as plaintiffs try to shoehorn as many standard business and non-business risks as possible into Marchand's 'essential and mission-critical' risk category."[18]

So, what does this mean for cyber-security-related board liability? Assessing cyber risks is critical, if not essential, for most organizations. Are cyber risk oversight failures likely to be the cases that break the duty of care standard related to board liability?

The following is a summary of two cases, both in 2021, where the Caremark standard intersected with claims involving cyber risk management:

- The first case involves two pension funds, which sued SolarWinds[19] when the company became a victim of a significant cyberattack and its stock dropped 40 percent. The lawsuits alleged the board did not receive relevant information from the committees responsible for cybersecurity, did not discuss cybersecurity at all in the two years leading up to the attack, and ignored warnings. Notwithstanding these allegations, in September 2022, the Delaware Court of Chancery found the plaintiffs "failed to plead specific facts to infer bad faith liability on the part of the directors." The court ruled that SolarWinds directors ensured that the company had at least a minimal reporting system about corporate risk, including cybersecurity, and further, that the board was not alleged to have ignored

16 *Ibid.*
17 *Marchand v. Barnhill*, 212 A.3d 805 (Del. 2019).
18 Jason J. Mendro, Andrew S. Tulumello, and Jason H. Hilborn, "Recent Application of Caremark: Oversight Liability," Harvard Law School Forum on Corporate Governance, August 16, 2019.
19 *Constr. Indus. Laborers Pension Fund v. Bingle*, C.A. No. 2021-0940-SG, (Del. Ch. September 6, 2022).

sufficient red flags of cyber threats to imply a conscious disregard of a known duty.[20]

- The second case involves a lawsuit against the Marriott International, Inc. board of directors for breach of its fiduciary duties, which was ultimately dismissed by the Delaware Court of Chancery. In 2015, Marriott announced its intent to acquire Starwood Hotels and Resorts Worldwide. However, despite knowing cybersecurity is a significant risk, the pre-acquisition board did not order any cybersecurity due diligence. Shortly after the acquisition, Starwood disclosed a malware infection and Marriott subsequently found lapses in cybersecurity controls. Due to the timing of the acquisition and breach, shareholders brought a lawsuit alleging the board violated their fiduciary duties by 1) failing to undertake cybersecurity and technology due diligence before the acquisition, 2) failing to implement adequate internal controls post-acquisition, and 3) failing to publicly acknowledge the data breach until November 2018, two months after Marriott first learned of the issue. However, the court found that under the stringent Caremark standard, the plaintiff's allegations fell short, failing to demonstrate that the Marriott directors "completely failed to undertake their oversight responsibilities, turned a blind eye to known compliance violations, or consciously failed to remediate cybersecurity failures."[21] The court further indicated that as regulatory frameworks advance to address cybersecurity practices, corporate governance, and not the law, must evolve to address these risks.[22]

In both cases, the court did not find the directors liable, suggesting Caremark claims will remain "the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment."[23] Nevertheless, it is worth noting a few interesting points:

- In the SolarWinds case, the court observed:

20 Fried Frank Harris Shriver & Jacobson LLP, "Court of Chancery Addresses Board Responsibility Under Caremark for Cybersecurity Risk—SolarWinds," Lexology.com, October 21, 2022.

21 Troutman Pepper, "Delaware Court of Chancery Highlights Seriousness of Cybersecurity Concerns While Maintaining High Standard for Caremark Claims," JDSupra.com, October 14, 2021.

22 Leo E. Strine, Jr., Kirby M. Smith, and Reilly S. Steel, "Caremark and ESG: Perfect Together: A Practical Approach to Implementing an Integrated, Efficient, and Effective Caremark and EESG Strategy," *Iowa Law Review*, July 30, 2020; pp. 1885 and 1893 (describing "the first principle of corporate law: corporations may only conduct lawful business by lawful means").

23 Mendro, Tulumello, and Hilborn, 2019.

  - The directors did not act in violation of "positive law." It "remains an open question" whether Caremark liability may be imposed for a board's failure to oversee business risk (such as cybersecurity risk unrelated to compliance with the law). How will this change when new cyber disclosure rules by the U.S. Securities and Exchange Commission (SEC) and other "positive laws" are in place?
  - The growing and consequential risks posed by cybersecurity threats, characterizing cybersecurity as a "mission-critical" risk for online providers.
  - Bad cybersecurity practices alone may not constitute bad faith, a core requirement under the Caremark standard.[24]
- In the Marriott case, the court acknowledged:
  - "[T]he corporate harms presented by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place."
  - While Marriot could have done more to prevent the data breach, the court pronounced "the difference between a flawed effort and a deliberate failure to act is one of extent and intent," and to adequately allege a Caremark claim the plaintiff must demonstrate the latter.[25]

An Important Healthcare Case to Watch

In *Cyber Risk and Patient Safety: A Tragic Call to Arms*,[26] we wrote about a lawsuit against an Alabama medical center that experienced a ransomware attack. Subsequently, a challenging baby delivery occurred, and nine months later, the baby died. Patient safety is a theme in the lawsuit, the plaintiffs asserting that "…the cyberattack on the hospital's computer and network systems implicated, and placed at risk, patient safety."

Under multiple causes of action cited, the lawsuit asserts departures from "the accepted standard of care" by "failing to have adequate rules, policies, procedures, and/or standards related to cyberattacks, including, but not limited to, specific standards associated with disclosure to the public, disclosure to physicians, appropriate assessment and risk analysis, training of hospital personnel, identification

24 Fried Frank Harris Shriver & Jacobson LLP, 2022.
25 Troutman Pepper, 2021.
26 Bob Chaput, "Cyber Risk and Patient Safety: A Tragic Call to Arms," Clearwater Compliance, October 6, 2021.

of potential hazards, and/or taking action regarding patients who are at risk when hospital electronic systems are not operational."[27]

The complaint names the hospital, a medical practice, a physician, and "A, B, C, D, E, F, and/or G, the persons, firms, or corporations responsible for delivery of medical care, nursing care, monitoring, diagnostics, and/or treatment of [baby's name] or [mother's name], at the times and places made the basis of this lawsuit; **H, I, J, and/or K, the persons, firms, and/or corporations who owned, operated, and/or controlled the hospital known** as Springhill Hospitals, Inc. d/b/a Springhill Memorial Hospital at the times and places made the basis of this lawsuit, all of whose true names and legal identities are otherwise unknown to plaintiffs at this time, but who will be added by amendment when ascertained, individually and jointly."[28]

Who are the unknown entities, H, I, J, and/or K? It's not a stretch to think that the C-suite and board could be named as owners, operators, or controllers of the business.

Three Other Relevant Cybersecurity Cases

Three other recent cases of interest that potentially implicate boards and possible failures to provide adequate cybersecurity oversight are those involving T-Mobile USA, Inc., Twitter, Inc., and Uber Technologies, Inc.

1. In November 2021, shareholders of T-Mobile filed a lawsuit alleging the board failed to "heed the red flags demonstrating the lack of cybersecurity over customer data."[29] The complaint focuses on the 2020 data breach, which affected 54 million customers and the subsequent investigation by the Federal Communications Commission (FCC). Importantly, the complaint alleges the board "utterly failed to fulfill its fiduciary duties to the company and its stockholders:"

   [T]he board was required to: 1) implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal identifying information of its customers is safe and secure, as represented; 2) implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the company, its stockholders, and customers by the storage of customer data and the "target"

27 Complaint at 39, *Kidd v. Springhill Hosp.*, 02-CV-2020-900171, June 4, 2020.
28 Complaint at 1, *Kidd v. Springhill Hosp.*, 02-CV-2020-900171, June 4, 2020.
29 *Litwin v. Sievert*, 2:21-cv-01599, (W.D. Wash. November 29, 2021).

such information posed to hackers and other malicious actors; and 3) take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the company's Web site allowed hackers to access customers' personal identifying information.[30]

This complaint points to the FCC investigation and resulting fine levied on T-Mobile to allege that the board was "long aware of" yet "failed to heed . . . red flags" related to the company's cybersecurity inadequacies.[31] While it is unclear whether the court will find the plaintiffs allege valid Caremark claims, this case should be closely monitored by boards and their counsel.

2. In August 2022, Peiter Zatko, Twitter's former head of security, filed whistleblower complaints with the SEC, the Federal Trade Commission, and the Justice Department alleging "extreme, egregious deficiencies by Twitter in every area of his mandate, including privacy, digital and physical security, platform integrity, and content moderation."[32] If investigations were to show the allegations to be true, this could represent serious privacy and security concerns for millions of Twitter users. Twitter subsequently reached a $7 million settlement with Zatko and a judge ruled that Musk could discuss security problems raised by Zatko during an October trial related to Musk's bid to buy Twitter. As for the executive team and board, it is yet to be determined whether there are governance and oversight implications and liability. As a recent SEC press release reminds us, whistleblower awards can range from 10 to 30 percent of the money collected when the monetary sanctions exceed $1 million and are regarded as a meaningful arrow in the SEC's enforcement quiver.[33] Will more CISOs come forward with similar allegations?

3. The October 2022 conviction of former Uber Chief Security Officer (CSO) Joe Sullivan has been characterized as "[T]he wrong result and a lost opportunity for the Federal Government to send a real message and set an example on cyber

30 *Ibid.*
31 Robert S. Velevis and Christina C. Koenig, "Caremark's Comeback Includes Potential Director Liability in Connection With Data Breaches," Sidley, January 26, 2022.
32 Sarah E. Needleman, "Twitter's Ex-Security Head Files Whistleblower Complaint on Spam, Privacy Issues," *The Wall Street Journal*, August 23, 2022.
33 U.S. Securities and Exchange Commission, "SEC Awards $20 Million to Whistleblower" (press release), November 28, 2022.

governance."[34] Sullivan was convicted of making payments to hackers in exchange for them signing non-disclosure agreements, which was seen as attempted concealment.[35] The complaint also alleged that Uber's then-CEO, Travis Kalanick, knew of the payments. The question of board oversight was raised as it was in the derivative lawsuits previously discussed; however, as Uber is private, there are no shareholders to file complaints against the board. Nevertheless, questions remain. How much did the board know? How would the Caremark standard have been applied in this case? We will never know.

→ Key Board Takeaways

- What sources are your C-suite and board using to keep abreast of relevant legal cases involving cyber risk management and cybersecurity?
- Have your C-suite executives and board members discussed their *fiduciary responsibility* for managing cyber risk?
- What is your C-suite's and board members' understanding of their *duty of care* concerning managing cyber risk?
- Have your C-suite executives and board members received effective training and education? If so, do they value the training received?
- Would your organization benefit from a session reviewing these and related legal cases by competent outside counsel and cyber risk management experts?
- What is the level of leadership by your executive team and degree of oversight by the board of your ECRM program?
- As a public company, how strong a position does your organization currently have in defense against the two prongs of a Caremark-based lawsuit?

New SEC Guidelines

At last, it seems the question of whether the SEC will order new cyber disclosure rules and other "positive laws" has been answered. In March 2022, the SEC issued a proposed rule titled "Cybersecurity Risk Management, Strategy, Governance,

34 Jody R. Westby, "Uber Trial: A Lost Opportunity For Cyber Governance," *Forbes*, October 8, 2022.
35 U.S. Attorney's Office, Northern District of California, "Former Chief Security Officer Of Uber Convicted Of Federal Charges For Covering Up Data Breach Involving Millions Of Uber User Records" (press release), Justice.gov, October 5, 2022.

and Incident Disclosure."[36] In it, the SEC describes its intention to require public companies to disclose whether their boards have members with cybersecurity expertise, and to disclose facts addressing:

- The board's oversight of cyber risk
- A description of management's role in assessing and managing cyber risks
- The relevant expertise of such management
- Management's role in implementing the registrant's cybersecurity policies, procedures, and strategies[37]

Regarding board oversight, the SEC will specifically require public companies to disclose:

- Whether the entire board, a specific board member, or a board committee is responsible for the oversight of cyber risks
- Processes by which the board is informed about cyber risks, and the frequency of its discussions on this topic
- Whether and how the board or specified board committee considers cyber risks as part of its business strategy, risk management, and financial oversight[38]

> While the courts in many of the foundational cases ultimately found in favor of the boards, these legal cases and the board's general responsibilities for risk, directors' fiduciary duty of care, and emerging national and international regulations and enforcement, should be seen as a harbinger for increased board liabilities in the courts.

Effective Compliance Programs: United States Sentencing Guidelines and Federal Prosecution of Business Organizations

As boards think about complying with the SEC's new cybersecurity risk management guidelines, they should also prepare for and guard against the risk of enforcement action by the SEC or prosecution by the Department of Justice (DOJ).

36 Keri Pearlson and Chris Hetner, "Is Your Board Prepared for New Cybersecurity Regulations?," *Harvard Business Review*, November 11, 2022.
37 *Ibid.*
38 *Ibid.*

In 1999, the DOJ issued the "Principles of Federal Prosecution of Business Organizations" (Principles) to articulate and standardize the factors to be considered by federal prosecutors in making charging decisions against corporations.[39] The DOJ announced that the existence and adequacy of an organization's compliance program and efforts to implement or improve an existing compliance program were among the factors that prosecutors would weigh when determining whether to prosecute an organization.[40] The advent of this new prosecutorial policy was based on the influence of Chapter Eight of the U.S. Sentencing Commission's Sentencing Guidelines, titled "Sentencing of Organizations."[41] This chapter instructs courts to determine an organization's culpability by considering six factors.[42] There are four aggravating factors "that increase the ultimate punishment of an organization," and two mitigating factors:

1. The existence of an effective compliance and ethics program
2. Self-reporting, cooperation, or acceptance of responsibility[43]

The fact that federal prosecutors are advised to use these mitigating factors is further encouragement for: 1) boards to focus on creating effective cybersecurity risk management programs as part of their existing compliance and ethics programs, and 2) boards to foster a system of accountability for cybersecurity breaches or failures. Doing so may not only prevent or detect misconduct by employees but may better position the company for leniency under the Principles or the Sentencing of Organizations' guidelines in a DOJ criminal investigation.[44] It is worth noting that although the Principles share many factors with the Sentencing Guidelines, the Principles differ from the Sentencing Guidelines in that they do not create a formulaic decision-making process for prosecutors.[45]

The Principles describe specific factors for prosecutors to consider in investigating a corporation, determining whether to bring charges, and negotiating a plea or other agreements.[46] There are three "fundamental questions" a prosecutor should ask

39 Beth A. Wilkinson and Alex Young K. Oh, "The Principles of Federal Prosecution of Business Organizations: A Ten-Year Anniversary Perspective," *Inside*, Fall 2009.
40 Kathleen C. Grilli, Kevin T. Maass, and Charles S. Ray, *The Organizational Sentencing Guidelines: Thirty Years of Innovation and Influence*, United States Sentencing Commission, 2022.
41 *Ibid.*
42 *Ibid.*
43 *Ibid.*
44 Wilkinson and Oh, 2009.
45 Wilkinson and Oh, 2009.
46 U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, June 1, 2020.

when investigating a corporation's compliance program—boards should consider these questions while assessing their cybersecurity risk management programs:

- Is the corporation's compliance program well designed?
- Is the program being applied earnestly and in good faith? (In other words, is the program adequately resourced and empowered to function effectively?)
- Does the corporation's compliance program work in practice?[47]

Knowledge of these factors can help boards ensure that the cybersecurity risk management aspects of their compliance programs are up to speed. Keeping these questions in mind as a board assesses its compliance program and its cybersecurity risk management efforts could ensure a more favorable outcome if a board's company became subject to a federal enforcement action. Finally, boards should note that the DOJ, in its "Evaluation of Corporate Compliance Programs," made a point to state:

The company's top leaders—the board of directors and executives—set the tone for the rest of the company. Prosecutors should examine the extent to which senior management have clearly articulated the company's ethical standards, conveyed and disseminated them in clear and unambiguous terms, and demonstrated rigorous adherence by example.[48]

Based on this statement, the DOJ will look for evidence of board leadership when evaluating a company's compliance program. It is very possible that the DOJ will look for the same evidence of board leadership when evaluating a company's cybersecurity risk management program, too.

Summary

All boards need to increase their oversight of cyber risk management. While the cases cited have primarily involved the boards of public companies in the U.S., others, such as private and not-for-profit companies, are not immune. While the courts in many of the foundational cases ultimately found in favor of the boards, these legal cases and the board's general responsibilities for risk, directors' fiduciary duty of care, and emerging national and international regulations and enforcement, should be seen as a harbinger for increased board liabilities in the courts.

47 *Ibid.*
48 *Ibid.*

As data breach law continues to develop, boards should act now to jump-start their enterprise cyber risk management efforts to establish, implement, and mature capabilities to manage these increased cyber risks and their attendant organizational and personal liabilities.

The Governance Institute thanks Bob Chaput, NACD.DC, MA, CISSP, HCISPP, CRISC, CIPP/US, C|EH, Executive Chairman and Founder, Andrew Mahler, JD, CIPP/US, CHC, CHPC, CHRC, Vice President, Privacy and Compliance, and Omenka Nwachukwu, JD, Privacy Consultant, Clearwater, for contributing this article. They can be reached at bob.chaput@clearwatercompliance.com, andrew.mahler@clearwatercompliance.com, and omenka.nwachukwu@clearwatercompliance.com.