Cybersecurity Developments and the Growing Role of Senior Executives and Directors

From the 2013 Target Corporation breach to this year's attacks on Primera Blue Cross and American Airlines Group Inc., the issue of cybersecurity has emerged at the forefront of risks to be confronted by corporations across a spectrum of industries.[1] Given the catastrophic risks and consequences that have emerged from recent cyberattacks and the litigation, regulatory, and enforcement trends that are driving the evolution of relevant legal standards, both senior executives and directors should be proactive in their oversight and monitoring of the implementation and continued refinement of their company's cybersecurity controls and processes.

I. Government Enforcement and Regulatory Attention to Cybersecurity

Multiple federal agencies have promulgated "checklists" or best practices for institutions to consider when addressing cybersecurity issues. In addition to being key indicators of government focus in this arena, these best practices may eventually form a *de facto* standard of care in cybersecurity. The ongoing Federal Trade Commission ("FTC") enforcement action against Wyndham Worldwide Corporation and various affiliated hotel entities (collectively, "Wyndham") provides helpful insight into this trend.

The FTC is currently pursuing cyber-related enforcement, pursuant to Section 5(a) of the Federal Trade Commission Act,[2] against Wyndham for "failure to maintain reasonable and appropriate data security for consumers' sensitive personal information."[3] The agency alleged that, despite Wyndham bearing "responsibil[ity] for creating information security policies for itself and its subsidiaries, . . . as well as [for] providing oversight of their information security programs," defendants failed to ensure implementation of such policies and procedures, to "remedy known security vulnerabilities," and to "employ reasonable measures to detect and prevent" breaches "or to conduct security investigations."[4] According to the FTC, these failures resulted in the exposure of over 619,000 consumer payment card account numbers, related fraudulent charges, and over $10.6 million in fraud loss.[5]

The FTC's case survived arguments in the district court that the FTC lacked "authority to assert an unfairness claim in the data-security context" and that such a claim must be preceded by formal regulations.[6] On August 24, 2015, the FTC's authority to undertake this enforcement action was affirmed by the Third Circuit Court of Appeals. The Circuit found both that (1) Wyndham's alleged cybersecurity shortcomings could constitute an unfairness claim and (2) Wyndham had sufficient notice of the meaning of Section 5(a) and its conduct could fall within the statute's scope.[7] Importantly, in determining the latter, the Third Circuit referred to

---

[1] *See* Kevin Granville, *9 Recent Cyberattacks Against Big Businesses*, N.Y. Times (Feb. 5, 2015) http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0; Ankit Ajmera & Jeffrey Dastin, *China-linked hackers attack American Airlines, Sabre systems: Bloomberg*, Reuters (Aug. 7, 2015), http://www.reuters.com/article/2015/08/07/us-american-airline-cyberattack-idUSKCN0QC16A20150807.

[2] 15 U.S.C. § 45(a) (Thomson Reuters 2015).

[3] First Amended Complaint for Injunctive and Other Equitable Relief at ¶ 1, *FTC* v. *Wyndham Worldwide Corp.*, No. 2:12-cv-01365, (D. Ariz. Aug. 9, 2012), ECF No. 28.

[4] *Id*. at ¶¶ 14, 24(c), (d), (h).

[5] *Id*. at ¶ 40.

[6] *FTC* v. *Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 607 (D.N.J. 2014) (denying Wyndham Hotel and Resort's motion to dismiss).

[7] *FTC* v. *Wyndham Worldwide Corp.*, 2015 WL 4998121, at *9, *13, *16 (3d Cir. Aug. 24, 2015).

the FTC's 2007 guidebook, *Protecting Personal Information: A Guide for Business*, in finding against Wyndham's fair notice challenge. According to the Circuit, the guidebook "describes a 'checklist[]' of practices that form a 'sound data security plan.'"[8] While none of the guidebook's practices are mandatory, the Circuit suggested that "[a]s the agency responsible for administering the statute, the FTC's expert views about the characteristics of a 'sound data security plan' could certainly have helped Wyndham" in addressing its conduct.[9] Not only does the decision validate the government's expansive view of the FTC Act and clear the way for further FTC enforcement in this arena, but it could elevate suggested "best practices" and other non-binding guidance to a status of a *de facto* standard of care in future litigation (government enforcement-based or otherwise).

Generally, federal legislation concerning officers' management and the board's oversight of information security within financial institutions has been around for some time. The Gramm-Leach-Bliley Act of 1999 (the "GLBA") provides the bedrock for government regulation over financial institutions in the cybersecurity arena.[10] The interagency guidance promulgated in accordance with the GLBA sets forth the responsibilities of the board in ensuring that an "information security program is developed, implemented, and maintained."[11] Senior management will be charged with the creation and implementation of such a program, and the Interagency Guidelines call on these officers to report to their boards on an annual basis (if not more regularly) on the "overall status" of their programs and their compliance with the guidelines.[12]

Moreover, agencies at the federal and state level have demonstrated that they view cybersecurity as a key consideration in corporate governance. New York has put specific focus on the banking industry; the Department of Financial Services informed institutions that its information technology/cybersecurity examination process will include assessments of "[c]orporate governance, including organization and reporting structure for cyber security related issues."[13] The SEC's Office of Compliance Inspections and Examinations also has cybersecurity on its radar, and earlier this year released information concerning its assessment of registered broker-dealers' and investment advisors' cybersecurity practices, including the "establish[ment of] cybersecurity governance, including policies, procedures, and oversight processes."[14]

Speaking more toward the directors' role, the SEC disclosure guidance on cybersecurity notes that disclosure duties and materiality requirements can include information regarding "cybersecurity risks and cyber incidents."[15] It has been suggested that, in considering enforcement actions, the SEC is focusing both on a company's "cyber security controls" and "how adequately companies are disclosing 'material' cyber events."[16]

---

[8] *Id*. at *14.

[9] *Id*. at *14-15.

[10] *See generally* 15 U.S.C. § 6801 (Thomson Reuters 2015).

[11] *See* Board of Governors of the Federal Reserve System, Interagency Guidelines Establishing Information Security Standards, http://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm#fn4r (hereinafter "Interagency Guidelines").

[12] *See* Interagency Guidelines.

[13] Letter from Benjamin M. Lawsky, Superintendent, New York Department of Financial Services, to All NYS-Chartered or Licensed Banking Institutions (Dec. 10, 2014), http://www.dfs.ny.gov/banking/bil-2014-10-10_cyber_security.pdf.

[14] SEC Office of Compliance Inspections and Examinations, National Exam Program Risk Alert, *Cybersecurity Examination Sweep Summary*, Vol. IV, Issue 4, at 1 (Feb. 3, 2015), http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

[15] SEC Division of Corporation Finance, *CF Disclosure Guidance: Topic No. 2 – Cybersecurity* (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[16] Sarah N. Lynch, *SEC on the Prowl for Cyber Security Cases: Official*, Reuters (Feb. 20, 2015), http://www.reuters.com/article/2015/02/20/us-sec-cyber-idUSKBN0LO28H20150220.

These types of activities and decisions are central to the responsibilities of corporate boards. This focus was made explicit last summer by SEC Commissioner Luis Aguilar, who stated that "ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk oversight responsibilities."[17]

As government regulation and enforcement activity develops in this area, so grows the expectation that senior corporate executives and directors will make cybersecurity a central part of their management and oversight duties and will utilize industry best practices.[18] As discussed above, non-mandatory FTC guidance was used by the Third Circuit in deciding the Wyndham appeal, thus increasing the stature of that guidance. Outside of the FTC, which published new business guidance this summer as part of its "Start With Security" initiative,[19] other potential standards are starting to take root. For example, the National Institute of Standards and Technology's 2014 "Cybersecurity Framework" is a voluntary set of industry standards and best practices for various critical infrastructure organizations, such as financial institutions.[20] More recently, the DOJ published a "Best Practices" cybersecurity guidance, which points to the NIST Framework in its Cyber Incident Preparedness Checklist.[21] The Checklist contemplates adopting certain best practices, such as "[c]reat[ing] an actionable incident response plan" and "[a]lign[ing] other policies (*e.g.*, human resources and personnel policies)" with that plan.[22] The SEC Division of Investment Management's Cybersecurity Guidance similarly provides suggestions for "funds and advisers . . . to consider in addressing cybersecurity risk," such as regular assessments of firm data, technology, potential risk and current security and governance; creation of a cyber-strategy; and implementation of that strategy via policy documentation and training.[23] As these and other cybersecurity best practices are further developed, implemented, and enforced, corporations that fail to adhere to them may become increasingly vulnerable to enforcement actions and civil litigation.

---

[17] Luis A. Aguilar, Commissioner, SEC, Speech at the NYSE "Cyber Risks and the Boardroom" Conference: *Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus* (June 10, 2014), http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#_ednref27.

[18] Cybersecurity regulations applicable to defense contractors are developing particularly rapidly. On August 26, 2015, the U.S. Department of Defense issued an interim rule requiring certain of its contractors and subcontractors to report a broad spectrum of cyber incidents. This rule took effect immediately rather than after a public comment period. *See* Emily Field, *DOD Issues New Cyber Reporting Rule For Contractors,* Law360 (Aug. 26, 2015), http://www.law360.com/articles/695612/dod-issues-new-cyber-reporting-rule-for-contractors.

[19] FTC, *FTC Kicks Off "Start With Security" Business Education Initiative* (June 30, 2015), https://www.ftc.gov/news-events/press-releases/2015/06/ftc-kicks-start-security-business-education-initiative; *see also* FTC, *Start With Security: A Guide For Business* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[20] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (hereinafter "NIST Framework"); *see also* The White House Office of the Press Secretary, "Presidential Policy Directive – Critical Infrastructure Security and Resilience" (Feb. 12, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (listing "Financial Services" as one of "16 critical infrastructure sectors").

[21] DOJ, Cybersecurity Unit, Computer Crime & Intellectual Property Section, Criminal Division, *Best Practices for Victim Response and Reporting of Cyber Incidents*, at 14 (Apr. 2015), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf (hereinafter "DOJ Best Practices"); *see also* Allison Grande, *DOJ's Cybersecurity Guide Opens Door to Liability Risks*, Law360 (May 4, 2015), http://www.law360.com/corporate/articles/651305?nl_pk=1d6be6c3-f8b9-45fc-bbf8-5e9076d794d7&utm_source=newsletter&utm_medium=email&utm_campaign=corporate.

[22] DOJ Best Practices at 14.

[23] SEC, Division of Investment Management, *Guidance Update: Cybersecurity Guidance*, No. 2015-02, at 1-2 (Apr. 2015), http://www.sec.gov/investment/im-guidance-2015-02.pdf.

II. Risk of Shareholder Litigation

Shareholders are similarly showing an increased interest in the intersection of cyber risk and corporate governance. In the wake of the cyberattack against Target, which compromised the data of approximately 110 million people and contributed to plummeting quarterly profits,[24] various shareholders filed derivative suits charging Target Corporation's "top-level executives and directors" with "breach of fiduciary duty and waste of corporate assets."[25] The defendants were alleged to have "failed to ensure that Target complied with even the most basic and fundamental industry standards for protecting consumer information that are common for large retail institutions[.]" Plaintiffs also alleged that various directors "breached their duty of loyalty" by "failing to implement a system of internal controls," "failing to oversee the (inadequate) internal controls that failed to protect" the data, and for "causing and/or permitting the Company to conceal the full scope of the data breach."[26] The outcome of this case will shape the contours of future derivative suits.

Several allegations from the Target complaint are especially notable, and should serve as warnings regarding improper cybersecurity management and governance. For example, plaintiffs allege not only that Target was informed of "suspicious activity involving payment cards used at its stores" by the Department of Justice – rather than discovering the breach itself – but Target's executives did not convey information about the breach to the then-Chairman of the Board/Chief Executive Officer until three days later, after the breach was confirmed.[27] The complaint further alleges Target waited a week after receiving initial information about the breach to disclose information to consumers, which ultimately turned out to be inaccurate.[28]

III. Executive Management and Board Oversight of Cyber Risks

Government, shareholders and civil litigants alike are looking to corporate officers and directors to tend to this critical issue. An institution's senior executives should take a hands-on approach to directing and monitoring the fortification and continuous enhancement of their company's cybersecurity processes and the development and implementation of a response plan that will mitigate damage in the event of a breach. Such enhancements will likely include assessing core business operations, identifying key personnel, and creating reporting procedures.[29] Senior management should ensure staff is trained appropriately on all procedures and protocols.[30]

Boards will play a critical role in overseeing all of these activities. A board's duty of loyalty includes a duty to oversee company risk,[31] and cybersecurity is among the most prominent risks facing corporations today. To meet this challenge, boards should proactively oversee and monitor the implementation, functioning, and

---

[24] Elizabeth A. Harris, *Data Breach Hurts Profit at Target*, N.Y. Times (Feb. 26, 2014), http://www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html (noting Target's profit "fell more than 40 percent in the fourth quarter").

[25] Verified Consolidated Shareholder Derivative Complaint for Breach of Fiduciary Duty and Waste of Corporate Assets at ¶ 1, *Davis* v. *Steinhafel,* No. 14-cv-00203-PAM-JJK (D. Minn. July 18, 2014), ECF No. 48. Among the supporting facts cited was Institutional Shareholder Services' recommendation that shareholders vote out seven Board members for their "failure to manage [cyber] risks." *Id.* at ¶ 125.

[26] *Id.* at ¶ 152.

[27] *Id.* at ¶¶ 15, 112-13. The Chairman also served as Target's president and as a director. *Id.* at ¶ 15.

[28] *Id.* at ¶¶ 115-120.

[29] *See* DOJ Best Practices at 1-2; *see also* NIST Framework at 8, 14-15.

[30] *See* DOJ Best Practices at 1.

[31] *See Stone ex rel. AmSouth Bancorp.* v. *Ritter*, 911 A.2d 362, 370 (Del. 2006).

continuous enhancement of cybersecurity protocols, policies, procedures, and controls. Boards would be well-served to periodically conduct independent assessments to "kick the tires" of the company's cybersecurity program to ensure that it reflects the latest legal, regulatory, and technological developments. A board should further ensure that it has an appropriate committee – for example, its audit committee or technology committee – charged with oversight of cyber risk. The board members or committee tasked with overseeing cybersecurity management should update the company's notification protocols to ensure (a) a system of regular updates about management processes and (b) that notices of any threats, breaches or attacks are communicated to responsible board members in a timely manner.

Senior management and board members alike should prepare for a potential crisis by regularly reviewing and updating their institution's cybersecurity breach protocol. In addition to investigating any attack, determining its scope, assessing the damage done, and instituting a recovery process, senior management will need to quickly apprise the board of the situation, and a board, in turn, should be involved as information is communicated to law enforcement authorities, employees, investors, customers, and the media. A disclosure protocol will ensure that critical information is circulated as appropriate and that disclosure determinations and public statements are properly vetted against internal governance polices and regulatory requirements.

Because cybersecurity can touch every aspect of a company's operation, senior executives and directors must consider the intersection of cybersecurity with other facets of company management, including staffing, budgeting, use of outside vendors, and potential acquisitions.

IV. Conclusion

The confluence of media attention, government enforcement, and shareholder litigation has rendered cybersecurity a critical and expanding part of corporate governance. The contours of this field are growing ever more complex as the actions taken by corporate executives and boards to counter cyber threats are increasingly scrutinized. All senior management personnel and corporate boards should fully incorporate cybersecurity concerns into day-to-day thinking and corporate oversight to be prepared for a cyberattack that is, regrettably, no longer a question of "if," but "when."

* * *

If you have any questions about the issues addressed in this memorandum or if you would like a copy of any of the materials mentioned, please do not hesitate to call or email David N. Kelley at 212.701.3050 or dkelley@cahill.com; Brockton B. Bosson at 212.701.3136 or bbosson@cahill.com; or Sarah M. Schoenbach at 212.701.3817 or sschoenbach@cahill.com.