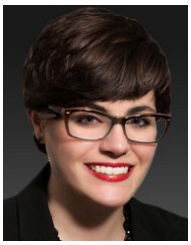
Fourth Quarter 2017 • Vol. XXX • Number 4

PLUS Journal *Reprint*
5353 Wayzata Blvd., Suite 600
Minneapolis, MN 55416-4758
phone 800.845.0778 or 952.746.2580

The mission of the Professional Liability Underwriting Society is to be the global community for the professional liability insurance industry by providing essential knowledge, thought leadership and career development opportunities.

PLUS
PROFESSIONAL LIABILITY UNDERWRITING SOCIETY
Journal
YOUR SOURCE FOR PROFESSIONAL LIABILITY EDUCATION AND NETWORKING



Andrew G. Lipton *is an associate at White and Williams LLP. represents foreign and domestic management liability insurers across multiple financial and specialty lines, including directors and officers liability, errors and omissions, employment practices liability, and representations and warranties liability. Andrew can be reached at liptona@whiteandwilliams.com.*

Laura Schmidt *is an associate at White and Williams LLP. Her practice includes cybersecurity and privacy law, insurance coverage litigation, bad faith litigation, and insurance contract disputes. Laura can be reached at schmidtl@whiteandwilliams.com.*

Breaching the D&O Firewall: The Rise of Cybersecurity Regulations for Businesses and the Future Effects on D&O Insurance

by Andrew G. Lipton & Laura Schmidt

For many D&O insurers, the risk of exposure posed by cybersecurity incidents involving their insureds has been unclear at best. Cybersecurity incidents, and the corresponding shareholder claims that follow, pose unique and challenging coverage issues under D&O insurance policies. Over the past several years, shareholder claimants have had only limited success with derivative lawsuits and securities class actions against companies' directors and officers after cybersecurity incidents, such as a data breach. These defense-friendly case decisions have shielded D&O insurers from potentially hefty jury verdicts and damages – to date.

However, D&O insurers should not get too comfortable. New developments have imposed additional responsibilities on company directors and officers in the cybersecurity area – most recently in sweeping regulations promulgated by the New York State Department of Financial Services. These new responsibilities suggest an evolving standard of care for a corporation's board and/or C-Suite officers with respect to preventing, developing, implementing, and maintaining cybersecurity policies and programs to mitigate, detect, and respond to cyber risks. Armed with an ever-evolving standard of care, corporate shareholders may be able to hold corporations and their management responsible for flawed or inadequate cybersecurity decision-making, which would inevitably lead to heightened exposure risks for D&O insurers in this volatile area. Based on prior D&O litigation trends, D&O insurers can expect that even a few litigation successes will inevitably lead to an increased rate of litigation by would-be shareholder plaintiffs.[2]

Fundamentals of D&O Insurance

The principal purpose of D&O insurance is to protect the personal assets of corporate directors and officers.[3] The D&O insurance policy typically contains three insuring agreements.[4] The "Side A" insuring agreement covers loss directly incurred by directors and officers that the corporation is not required or permitted to pay as indemnification to the directors and officers.[5] The "Side B" insuring agreement covers loss the corporation pays, or is required or permitted to pay, as indemnification to its directors and officers.[6] The 'Side C" insuring agreement covers loss incurred by the corporation itself, commonly only for securities claims if the insured is a public corporation.[7] At its core, directors and officers liability is grounded in corporate decision-making. The quality and integrity of corporate decision-making is constantly being tested by new rules and regulations governing corporate compliance. Once a new set of rules enters the C-Suite, the prospect of loss incurred due to corporate actions, or lack thereof, crosses a significant threshold.

Lack of Success from Early Shareholder Lawsuits

Until recently, courts have been hesitant to find that directors and officers were remiss in their fiduciary duties with respect to preparing for, preventing or responding to a cybersecurity incident. For example, in 2016, a Minnesota federal judge granted motions to dismiss filed by Target Corporation's executives, directors and the board of director's special litigation committee after the special litigation committee issued a 91-page report concluding that Target should not pursue derivative claims against officers and directors based on the company's 2013 cyber breach incident,[8] which affected approximately 110 million Target customers.[9] Had the court allowed the Target derivative litigation to move forward, the potential exposure to Target's directors and officers and to Target's D&O insurers would have been enormous, given the magnitude of the data breach.

In another notable D&O case, shareholders for Wyndham Worldwide Corporation initiated a shareholder derivative lawsuit against certain directors and officers of the company, relating to three cyber breaches that the company suffered between April 2008 and January 2010.[10] After an investigation was commenced by the

Federal Trade Commission, a Wyndham shareholder issued a letter to the board of directors of Wyndham demanding that a lawsuit be commenced against the board for its allegedly inept data security practices.[11] In the complaint, the plaintiff shareholder alleged the company and its subsidiaries failed to take reasonable steps to protect customers' personal and financial information in a secure manner, and failed to timely disclose the cyber breaches in the Company's financial filings.[12] The plaintiff further alleged that the defendants' failure to protect against cyber breaches severely damaged the company and its reputation and resulted in an enforcement action by the FTC.[13] After reviewing the demand (and other similar demands which were issued by other shareholders), the board had decided not to bring the lawsuit because it judged that the demand was not "well-grounded."[14]

The Court, applying Delaware law, granted the defendants' motion to dismiss, concluding that the board's refusal to pursue the plaintiff's demand for a lawsuit was a good-faith exercise of business judgment made after a reasonable investigation.[15] The court concluded that due to the "ample information" the board had at its disposal when it rejected the derivative plaintiff's demand, and the "numerous steps" the board took to familiarize itself with the subject, the plaintiff had failed to make a showing that the board's investigation of the cyber security incidents was unreasonably designed or conducted.[16] In particular, the court noted that between 2008 and 2012, the Wyndham board engaged in discussions about cyber security and proposed security enhancements at fourteen separate board meetings, and had hired various technology firms to investigate the breaches and provide recommendations for enhancing the company's security. The board implemented those recommendations.[17]

The Court agreed with the board's stated reasons for demand refusal, namely that commencing a suit would impair Wyndham's ability to defend against the FTC suit. Thus, the court concluded that Wyndham's board "had a firm grasp of Plaintiff's demand when it determined that pursuing it was not in the corporation's best interest."[18]

Settlements and the Rise of Regulations: A Standard of Care Begins to Take Shape

While the shareholders in the *Target* and *Wyndham* suits were unsuccessful in successfully pleading shareholder derivative complaints, D&O insurers already have paid substantial defense costs associated with these unsuccessful derivative claims. Additionally, insurers should anticipate the potential for coverage of future settlements of D&O cases involving cybersecurity issues in light of more rigorous regulatory standards that companies are expected to adopt.

For example, the Securities and Exchange Commission and the New York Department of Financial Services have both announced their intentions to hold directors and officers to a responsible standard when it comes to preventing and responding to cybersecurity incidents.

In the SEC's Examination Priorities, published on January 12, 2017, the SEC warned publicly traded companies that it will be investigating cybersecurity practices with higher scrutiny.[19] Specifically, the SEC states that "[i]n 2017, we will continue our initiative to examine for cybersecurity compliance procedures and controls, including testing and implementation of those procedures and controls."[20]

In early 2017, the New York State Department of Financial Services ("NYDFS") enacted game-changing regulations which establish new standards for corporate cybersecurity practices.[21] The rules, which went into effect on March 1, 2017, apply to any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.[22] Under the NYDFS regulations, companies regulated by NYDFS are required to establish a cybersecurity policy, maintain a cybersecurity program, and designate a Chief Information Security Officer (CISO) responsible for overseeing and implementing the cybersecurity program and enforcing the cybersecurity policy.[23] The NYDFS regulations require the company's CISO to report, in writing at least, annually to the Covered Entity's board of directors or equivalent governing body on the company's cybersecurity program and material risks.[24]

However, the most significant parts of the NYDFS cybersecurity regulations for D&O insurers are the requirements imposed on "Senior Officers," defined as individuals responsible for the management, operations, security, information systems, compliance and/or risk. Senior officers or the Company's board of directors must approve the written cybersecurity policies and procedures developed by the company.[25] Additionally, senior officers must certify on an annual basis compliance with the NYDFS requirements.[26]

These regulations are designed to shift the burden of cybersecurity prevention, detection and response to the private sector as a matter of public policy.[27] This dynamic shift arguably adds weight to the level of scrutiny that will be applied to corporations and their management who do not comply with these regulations.[28] As described in the introduction of the NYDFS cybersecurity statute, "[s]enior management must take this issue seriously and be responsible for the organization's cybersecurity program…A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its customers. It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program."[29]

In addition to these regulations, the increase in data breach litigation and recent high profile settlements have further fleshed out the responsibilities of corporate management. For example, in August 2015, shareholders filed a derivative complaint against Home Depot alleging that certain directors and officers failed to institute internal controls sufficient to oversee the risks that Home Depot faced in the event of a data breach.[30] The court ultimately sided with Home Depot's board of directors, concluding that while in hindsight Home Depot's implementation of a data security plan was too slow, the plan would not have fixed all of Home Depot's security issues. A corporate director's decisions need only be reasonable, not perfect.[31] While an appeal of the dismissal was pending, the parties reached a settlement. Pursuant to the settlement agreement, Home Depot agreed to adopt certain cyber-security related corporate governance reforms, which would require Home Depot's board of directors, in part, to:

- document the duties and responsibilities of the Chief Information Security Officer ("CISO");
- periodically conduct table-top cybersecurity exercises;
- monitor and periodically assess key indicators of compromise on computer network endpoints;
- maintain and periodically assess the company's partnership with a dark web

mining service to search for confidential Home Depot information;

- maintain an executive-level committee focused on the company's data security;
- receive periodic reports from management regarding the amount of the company's IT budget and what percentage of the IT budget was spent on cybersecurity measures;
- maintain an Incident Response Team and an Incident Response Plan;
- maintain membership in at least one Information Sharing and Analysis Center ("ISAC") or Information Sharing and Analysis Organization ("ISAO"); and
- retain their own IT, data and security experts and consultants as deemed necessary.[32]

In the motion before the court to approve the settlement, the plaintiffs asserted that these corporate governance reforms provided "clear roles and responsibilities over data security" and called for Home Depot to "proactively monitor external sources, share information about potential threats and maintain a response plan, all of which increases accountability and oversight over the Company's data security systems."[33]

Home Depot's settlement is significant for D&O coverage for two reasons. First, the settlement identifies clear practices and policies that directors and officers are likely to implement to respond to a data breach. As more of these settlement agreements are hashed out, a clearer picture will form regarding the standard of care that directors and officers will be held to when preventing and/or responding to a data breach. Second, the Home Depot settlement raises the question of whether the adoption of a heightened compliance regime as part of a settlement creates coverage or funding obligations under a D&O insurance policy.

Takeaways: The Nature of Cyber Risk Assessment for D&O Underwriters Must Evolve

Cases similar to *Wyndham* and *Home Depot* will become more commonplace as the nature and severity of cyber risk evolves. However, D&O underwriters can no longer rely on the relative inexperience of courts, or the lack of controlling precedent, to assess the level of risk a certain insured poses due to the possibility of cyberattacks. Previously, as exhibited by the courts' reasoning in these cases, cyber losses only *potentially* implicated D&O exposure. Going forward, it can be expected that the NYDFS cybersecurity regulations (and similar state and federal regulations which may follow) will act to un-blur these lines by delineating specific prevention, detection and response duties for corporate management. This development will effectively place a corporation's D&O insurance program directly in the cross-hairs when corporate management fails to live up to those heightened duties. For every cyber loss a corporate insured is exposed to, the inquiry will immediately turn to whether the board or C-Suite of that corporation insured adequately complied with the given cybersecurity regulations. D&O insurers should be forewarned.

Endnotes

1 The authors wish to extend a special thanks to John McCarrick, chair of the Directors and Officers Group of White and Williams LLP, as well as Joshua Mooney and Jay Shapiro, co-chairs of the Cyber Law & Data Protection Group of White and Williams LLP, for their guidance and insight during the drafting of this article.

2 Whether D&O insurers can charge additional premiums that reflect this heightened risk in the current, highly-competitive underwriting environment is another story, and beyond the scope of this article.

3 *See* 4-26 New Appleman on Insurance Law Library Edition § 26.01.

4 *See* 3-37 New Appleman Insurance Law Practice Guide § 37.02.

5 *Id.* **6** *Id.* **7** *Id.*

8 *See generally* Mary Davis, et al. v. Gregg W. Steinhafel, et al., United States District Court for the District of Minnesota, Lead Case No. 14-cv-203 (PAM/JJK), Order (Filed Jul. 7, 2016); Mary Davis, et al. v. Gregg W. Steinhafel, et al., United States District Court for the District of Minnesota, Civil Action No. 14-cv-00203 (PAM-JJK), Memorandum of Law of the Special Litigation Committee of the Board of Directors of Target Corporation in Support of its Motion for Approval and Dismissal (Filed May 6, 2016).

9 *See* Jonathan Stempel and Nandita Bose, *Target in $39.4 million settlement with banks over data breach*, Reuters (Dec. 2, 2015), http://www.reuters.com/article/us-target-breach-settlement-idUSKBN0TL20Y20151203.

10 See Palkon v. Holmes, Civil Action No. 2:14-CV-01234 (SRC), 2014 U.S. Dist. LEXIS 148799, *2 (D.N.J. Oct. 20, 2014).

11 *See id.* **12** *See id.* at *2-*5. **13** *See id.*

14 *See id.* **15** *See generally id.* **16** *See id.* at *12.

17 *See id.* **18** *See id.* at *15.

19 https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2017.pdf.

20 *See id.* **21** *See* 23 NYCRR §§ 500.00-500.23.

22 Id. **23** Id. **24** Id. **25** Id.

26 Id. **27** Id. **28** Id.

29 23 NYCRR §§ 500.00.

30 *See In Re The Home Depot, Inc. Shareholder Derivative Litigation*, United States District Court for the Northern District of Georgia, Atlanta Division, Civil Action File No. 1:15-CV-2999-TWT, Opinion and Order (Nov. 30, 2016).

31 *See id.* (quoting Lyondell Chemical Co. v. Ryan, 970 A.2d 235, 243 (Del. 2009)).

32 *See http://www.dandodiary.com/wp-content/uploads/sites/265/2017/05/home-depot-settlement.pdf*

33 *See id.*