2018 MIDWEST LEGAL CONFERENCE ON PRIVACY AND DATA SECURITY

Advising the Board of Directors on Privacy and Data Security

Melissa Krasnow, Partner, VLP Law Group LLP, mkrasnow@vlplawgroup.com

Mark Abbott, Chief Legal Officer, Atomic Data, LLC, mark@atomicdata.com

Michael Johnson, Honeywell/James J. Renier Chair in Security Technologies, University of Minnesota Technological Leadership Institute, mpj@umn.edu

SLIDES

LESSONS FROM SHAREHOLDER DERIVATIVE LAWSUITS

2017 SECURITIES CLASS ACTION LAWSUITS INVOLVING DIRECTORS & OFFICERS

NATIONAL ASSOCIATION OF CORPORATE DIRECTORS
CYBER-RISK OVERSIGHT HANDBOOK FOR DIRECTORS

NATIONAL ASSOCIATION OF CORPORATE DIRECTORS
2017-2018 NACD PUBLIC COMPANY GOVERNANCE SURVEY

NEW REGULATION

NEW LEGISLATION

ADDITIONAL RESOURCES

LESSONS FROM SHAREHOLDER DERIVATIVE LAWSUITS

Wyndham Shareholder Derivative Lawsuit (Delaware law)

Caremark requires that a corporation's "directors utterly failed to implement any reporting or information system ... [or] consciously failed to monitor or oversee its operations thus disabling themselves from being informed." Stone v. Ritter, 911 A.2d 362, 370 (Del. 2006). Yet Plaintiff concedes that security measures existed when the first breach occurred, and admits the Board addressed such concerns numerous times. (Compl. ¶¶ 46, 62, 63). The Board was free to consider such potential weaknesses when assessing the lawsuit.

Palkon v. Holmes, 2014 U.S. Dist. LEXIS 148799 (D.N.J. Oct. 20, 2014).

LESSONS FROM SHAREHOLDER DERIVATIVE LAWSUITS (CON'T)

Home Depot Shareholder Derivative Lawsuit (Delaware law)

…the [p]laintiffs essentially need[ed] to show with particularized facts beyond a reasonable doubt that a majority of the Board faced substantial liability because it consciously failed to act in the face of a known duty to act. This is an incredibly high hurdle for the [p]laintiffs to overcome, and it is not surprising that they fail[ed] to do so.

In re The Home Depot, Inc. Shareholder Derivative Litigation, No. 1:15-CV-2999 (N.D. Ga. Nov. 30, 2016).

LESSONS FROM SHAREHOLDER DERIVATIVE LAWSUITS (CON'T)

Home Depot Shareholder Derivative Lawsuit (Delaware law)

...'Directors' decisions must be reasonable, not perfect.' Lyondell, 970 A.2d at 243. While the Board probably should have done more, '[s]imply alleging that a board incorrectly exercised its business judgment and made a 'wrong' decision in response to red flags. . . .is not enough to plead bad faith.' Melbourne Mun. Firefighters' Pension Trust Fund on Behalf of Qualcomm, Inc. v. Jacobs, C.A. No. 10872-VCMR (Del. Ch. Aug. 1, 2016). Id.

In re The Home Depot, Inc. Shareholder Derivative Litigation, No. 1:15-CV-2999 (N.D. Ga. Nov. 30, 2016).

LESSONS FROM SHAREHOLDER DERIVATIVE LAWSUITS (CON'T)

Home Depot Shareholder Derivative Lawsuit Settlement (Delaware law)

Home Depot's settlement of the shareholder derivative lawsuit requires implementation of 9 corporate governance reforms, among other things:

1. Documenting the CISO's duties and responsibilities and providing this to shareholder counsel.

2. Periodically conducting table top cyber exercises to validate its processes and procedures, testing the readiness of its response capabilities, raising organizational awareness, training its personnel and creating remediation plans for issues and problem areas.

3. Monitoring and periodically assessing key indicators of compromise on computer network endpoints.

LESSONS FROM SHAREHOLDER DERIVATIVE LAWSUITS (CON'T)

Home Depot Shareholder Derivative Lawsuit Settlement (Delaware law)

4. Maintaining and periodically assessing partnership with a dark web mining service to search for Home Depot information.

5. Maintaining an executive-level ‘‘Data Security and Privacy Governance Committee” or comparable executive-level committee focused on data security and documenting the duties and responsibilities of such committee and providing such documentation to shareholder counsel.

6. Receiving periodic reports from management regarding the amount of Home Depot’s IT budget and the percentage of budget spent on cybersecurity measures.

LESSONS FROM SHAREHOLDER DERIVATIVE LAWSUITS (CON'T)

Home Depot Shareholder Derivative Lawsuit Settlement (Delaware law)

7. Maintaining the incident response team and incident response plan to address crises or disasters and periodically re-evaluating the plan.

8. Maintaining membership in at least one Information Sharing and Analysis Center (ISAC) or Information Sharing and Analysis Organization (ISAO).

9. Authorizing the board and audit committee to retain their own IT and data and security experts and consultants as they deem necessary.

In re The Home Depot, Inc. Shareholder Derivative Litigation, Lead Case No. 15-CV-2999-TWT (N.D. Ga. Oct. 2017).

LESSONS FROM SHAREHOLDER DERIVATIVE LAWSUITS (CON'T)

Target Shareholder Derivative Lawsuit (Minnesota law)

A Special Litigation Committee established by Target's board of directors pursuant to Minnesota law issued a report to Target's board that concluded it would not be in the best interests of Target to pursue any of the alleged derivative claims and that the derivative action and the alleged derivative claims should be dismissed. The court granted the motions to dismiss the derivative action of the Special Litigation Committee, Target and the defendants and ordered that the derivative action be dismissed with prejudice.

In re Target Corp. Shareholder Derivative Litigation, No. 0:14-CV-00203 (D. Minn. July 7, 2016).

2017 SECURITIES CLASS ACTION LAWSUITS INVOLVING DIRECTORS & OFFICERS

In re Yahoo! Inc. Securities Litigation, No. 5:17-cv-00373 (N.D. Ca.)

Kuhns v. Equifax Inc., No. 1:17-cv-03463 (N.D. Ga.)

Sgarlata v. PayPal Holdings, Inc., No. 3:17-cv-06956 (N.D. Ca.)

Ramnath v. Qudian Inc., No. 1:17-cv-09741 (S.D.N.Y.)

Voluntary dismissal without prejudice. Brock v. Equifax Inc., No. 1:17-cv-04510 (N.D. Ga. Dec. 22, 2017).

NATIONAL ASSOCIATION OF CORPORATE DIRECTORS
CYBER-RISK OVERSIGHT HANDBOOK FOR DIRECTORS
AT HTTPS://WWW.NACDONLINE.ORG/CYBER

Applicable to public, private and nonprofit company boards.

Organized around five principles to consider in seeking to enhance oversight over cyber risks.

Questions for directors to ask management about cybersecurity, to assess board's "cyber literacy" and to assess board's cybersecurity culture.

See also: https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/cgri-closer-look-69-cybersecurity-experise-boardroom.pdf

NATIONAL ASSOCIATION OF CORPORATE DIRECTORS
2017-2018 NACD PUBLIC COMPANY GOVERNANCE SURVEY

According to the following percentages of respondents, management representatives reporting to the board about state of cybersecurity include: CIO (67%), Head of Internal Audit (46%), CEO (42%), CISO (39%) and General Counsel (28%).

22% of respondents were dissatisfied with the quality of cyber risk information provided to the board by management.

According to the following percentages of respondents, reasons for dissatisfaction are that the information: does not provide enough transparency about performance issues (44%) or allow for effective benchmarking (41%), is difficult to interpret (29%) and is not timely enough or does not clearly connect to the firm's strategy (each 24%).

NATIONAL ASSOCIATION OF CORPORATE DIRECTORS
2017-2018 NACD PUBLIC COMPANY GOVERNANCE SURVEY (CON'T)

Cyber risk oversight practices performed by the board over the last 12 months include:

Participated company response plan test (14%), conducted postmortem review after actual or potential incident (24%) and reviewed company's response plan in case of a breach (61%).

Reviewed scope of cyber coverage in the case of an incident (40%), discussed legal implications of a breach (38%), attended continuing education events on cyber risk (33%) and leveraged external advisors to understand the risk environment (31%).

NEW REGULATION

Can our legal and compliance officers identify all existing regulations that apply to cyber and information security, and do they understand which new mandates are under consideration or in development?

Source: 2018 Governance Outlook: Projections on Emerging Board Matters at https://www.nacdonline.org/outlook?mkt_tok=eyJpIjoiTkdJM01EZGxNVGswTWpGaCIsInQiOiJcL1RFQ2NxYkptVHMzV01cL2I1QXNkQXF1dTlrMUJlNVdRdEtxSVpOWDBiQ1VlTVBiN2dSd3RvRTEyZ3pQU1FxaHhXWXpaME1VXC9LYVl4YlwveVBFYVRcL0ZMcktGMFwvM08zNDRaMTd6QTRzZFwvbGlnWUw1czJ3TWVHRFE3RHM0TDg0ZEIifQ%3D%3D

NEW REGULATION (CON'T)

European Union (EU) General Data Protection Regulation (GDPR) at http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

The UK's Information Commissioner's Office (ICO) has described the legislation [which comes into effect on May 25, 2018] as 'an evolution in data protection regulation, not a burdensome revolution'….

Even so, the regulation is a gear-shift in data protection, requiring greater transparency from handlers of personal data, enhancing the rights of individuals over their information and increasing the fines that can be levied for data protection breaches.

Source: Will GDPR prove to be a trick or a treat for boards? at https://www.icsa.org.uk/knowledge/governance-and-compliance/features/data-protection-gdpr-icsa-guidance

NEW REGULATION (CON'T)

NEW YORK'S CYBERSECURITY REGULATION (23 NYCCR PART 500) AT HTTP://DFS.NY.GOV/LEGAL/REGULATIONS/ADOPTIONS/DFSRF500TXT.PDF

Section 500.03 Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems….

Section 500.04 Chief Information Security Officer. (b) Report. The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. The CISO shall report on the Covered Entity's cybersecurity program and material cybersecurity risks…..

APPENDIX A (Part 500)
(Covered Entity Name)
February 15, 20
Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations
The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:
(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;
(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity) as of (date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended (year for which Board Resolution or Compliance Finding is provided) complies with Part ___.
Signed by the Chairperson of the Board of Directors or Senior Officer(s)
(Name) Date: _____
[DFS Portal Filing Instructions]

NEW LEGISLATION

FEDERAL DATA SECURITY AND BREACH NOTIFICATION ACT (S. 2179)

(f) CONCEALMENT OF BREACHES OF SECURITY.—
(1) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following:
"§ 1041. Concealment of breaches of security involving personal information
"(a) IN GENERAL.—Any person who, having knowledge of a breach of security and of the fact that notification of the breach of security is required under the Data Security and Breach Notification Act, intentionally and willfully conceals the fact of the breach of security, shall, in the event that the breach of security results in economic harm to any individual in the amount of $1,000 or more, be fined under this title, imprisoned for not more than 5 years, or both.
"(b) PERSON DEFINED.—For purposes of subsection (a), the term 'person' has the same meaning as in section 1030(e)(12) of this title.
"(c) ENFORCEMENT AUTHORITY.—
"(1) IN GENERAL.—The United States Secret Service and the Federal Bureau of Investigation shall have the authority to investigate offenses under this section.
"(2) CONSTRUCTION.—The authority granted in paragraph (1) shall not be exclusive of any existing authority held by any other Federal agency.".
(2) CONFORMING AND TECHNICAL AMENDMENTS.—The table of sections for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

"1041. Concealment of breaches of security involving personal information.".

ADDITIONAL RESOURCES

Home Depot Builds a Data Breach Settlement Blueprint:
https://www.bna.com/home-depot-builds-n57982087389/

Equifax Data Breach May Prompt Shareholder Derivative Suit:
https://www.bna.com/equifax-data-breach-n57982087848/

See also:
https://www.vlplawgroup.com/attorneys/melissa-krasnow/