ALSTON &BIRD

Advising the C-Suite and Boards of Directors on Cybersecurity

February 11, 2015

Agenda

- Introductions / Administrative
- Cybersecurity risk legal landscape
  - Cyber threats
  - Legal risks in the aftermath of a breach
- The role of the board in cybersecurity
  - Board duties
  - Shareholder demands and derivative actions
  - Cyber risk oversight – best practice guidance and regulator's view
- Cyber breach response

Presenters

Jessica Corley
Partner
Securities Litigation

Scott Ortwein
Partner
Corporate Transactions

Kim Peretti
Partner
Privacy & Data Security

Jim Harvey
Partner
Privacy & Data Security

Moderator

The Cyber Threat Landscape

The New York Times

U.S. Said to Find North Korea Ordered Cyberattack on Sony

From Exploitation to Disruption to Destruction

Forbes

JP Morgan Chase Warns Customers About Massive Data Breach

InformationWeek DARKReading

FBI Briefs Bank Executives On DDoS Attack Campaign

Fluid Dynamics of Cyber Risk

- Increasingly hard to keep breaches private irrespective of legal obligations (or control the disclosure).
- Shift from smash-and-grab to deep and prolonged access.
- Investigations produce uncertain results, increasing risk exposure.
- Detection can occur months or years after initial compromise.
- Evidence often not available, leaving victims unable to "prove the negative."
- Risks:
  - Reputational
  - Regulatory
  - Litigation
  - Payment Cards

Board Duties Regarding Cybersecurity

- Cybersecurity is becoming a priority issue for boards due to large number of breaches and extensive press activity.
- State law governs the board's duties.
  - Assume Delaware law for purposes of this presentation.
- Directors:
  - Do not have to become experts on cybersecurity, and
  - Are permitted (and expected) to rely on information and reports from management and others regarding cybersecurity and cyber risk.
- The Board should:
  - Inform itself regarding cybersecurity risk,
  - Be comfortable that the company has appropriate controls in place to manage that risk, and
  - Monitor controls periodically to ensure that they are functioning as intended and that issues are being identified and addressed.

Practical Metrics for Board Reporting and Cyber Issues

- How frequently does the Board receive reports on cybersecurity and cyber risk?
  - What reporting on cyber issues has occurred in the last twelve months?
- Do the reports go to:
  - The full Board?
  - The Audit Committee?
  - The Risk Committee?
- Who reports? How? In what form?
  - Incident Readiness and Planning
  - Threat Intelligence
  - Cyber Security Governance
  - Internal and External Controls
- Minutes of the Board or Committee Meetings?
  - Appropriate detail

The SEC is Focused on Boards and Cybersecurity

U.S. Securities and Exchange Commission

ABOUT | DIVISIONS | ENFORCEMENT | REGULATION | EDUCATION | FILINGS

ewsroom
ress Releases
ublic Statements
peeches
estimony
otlight Topics
edia Kit

SPEECH

Boards of Directors, Corporate Governance and Cyber Risks: Sharpening the Focus

Commissioner Luis A. Aguilar

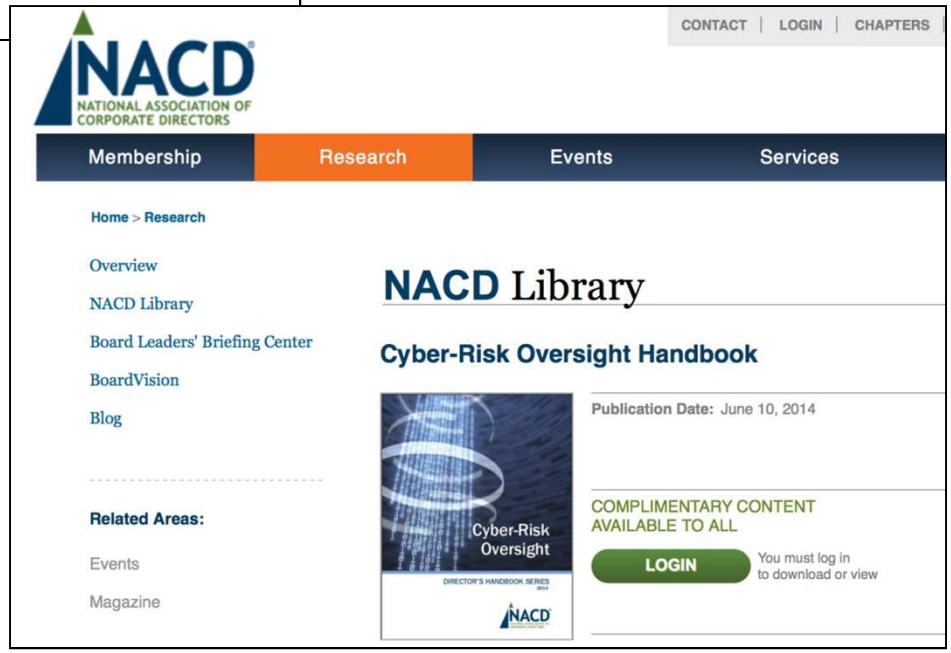
"Cyber Risks and the Boardroom" Conference
New York Stock Exchange
New York, NY

June 10, 2014

Third Party Guidance on Boards and Cyber Risk

FFIEC CYBERSECURITY ASSESSMENT GENERAL OBSERVATIONS

During the summer of 2014, Federal Financial Institutions Examination Council (FFIEC) members[1] piloted a cybersecurity examination work program (Cybersecurity Assessment) at over 500 community financial institutions to evaluate their preparedness to mitigate cyber risks. This document presents general observations from the Cybersecurity Assessment about the range of inherent risks and the varied risk management practices among financial institutions and suggests questions for chief executive officers and boards of directors to consider when assessing their financial institutions' cybersecurity and preparedness. This document should not be construed as guidance. Related guidance appears at the end of the document.



Beware – Section 220 Demands

FindLaw ▸ Codes and Statutes ▸ Delaware Code ▸ Title 8 ▸ Chapter 1 ▸ Subchapter VII ▸ Section 220

DEL CODE § 220 : Delaware Code - Section 220: INSPECTION OF BOOKS AND RECORDS

Search DEL CODE § 220 : Delaware Code - Section 220: INSPECTION OF BOOKS AND RECORDS

Section 220 Demands (cont.)

- It is common to receive demands for investigation and books and records by shareholders in the post breach context.

Investigation

- Shareholder will demand that the board investigate the breach and take action against any wrongdoers.
- Board hires counsel to conduct investigation.

Books and Records

- Entitled to receive board materials related to cybersecurity and independence of the members of the board.
- Will negotiate a non-disclosure agreement before producing documents.
- Shareholder will either (1) go away, (2) file a lawsuit demanding additional materials, or (3) file a derivative lawsuit.

Shareholder Derivative Suits

Target Execs Slapped With Investor Suit Over Data Breach

By **Jamie Santo**

Law360, New York (January 29, 2014, 10:53 PM ET) -- A Target Corp. investor launched a derivative suit in Minnesota federal court Wednesday, to hold the retailer's top brass liable for damage caused by the holiday season data breach that saw hackers steal personal and financial information from tens of millions of customers.

Filed by shareholder Maureen Collier, the complaint alleges that Target's board and top executives harmed the company financially by failing to take adequate steps to prevent the cyberattack then by subsequently providing customers with incomplete and misleading information about the extent of the...

Recent Shareholder Derivative Litigation

- Typical allegations against officers and directors in derivative litigation:
  - Breach of the duty of loyalty and care,
  - Wasted corporate assets, and
  - Were unjustly enriched by the compensation they received while breaching their fiduciary duties.
- Cannot prevent these lawsuits, but best defense is:
  - Regular reporting and review of controls,
  - Appropriate governance, and
  - Confirmation by the Board that the organization is staying abreast of evolving threats and adjusting its security posture accordingly.
- Very early in the life cycle of these cases – final resolution is difficult to predict today.

Wyndham Litigation / Conflicts of Interest

WOLLMUTH MAHER & DEUTSCH LLP
David H. Wollmuth (DW-9618)
dwollmuth@wmd-law.com
Frederick R. Kessler (FK-8168)
fkessler@wmd-law.com
One Gateway Center
Newark, NJ 07102
(973) 733-9200

Attorneys for Plaintiff

[Additional Counsel on Signature Page]

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

DENNIS PALKON, Derivatively on Behalf of WYNDHAM WORLDWIDE CORPORATION, Plaintiff, v. STEPHEN P. HOLMES, ERIC A. DANZIGER, SCOTT G. MCLESTER, JAMES E. BUCKMAN, MICHAEL H. WARGOTZ, GEORGE HERRERA, PAULINE D.E. RICHARDS, MYRA J. BIBLOWIT, BRIAN MULRONEY, STEVEN A. RUDNITSKY, and DOES 1-10, Defendants, -and- WYNDHAM WORLDWIDE CORPORATION, a Delaware corporation, Nominal Defendant.	Case No.: VERIFIED SHAREHOLDER DERIVATIVE COMPLAINT FOR BREACH OF FIDUCIARY DUTY, WASTE OF CORPORATE ASSETS, AND UNJUST ENRICHMENT DEMAND FOR JURY TRIAL

Preventive Maintenance – Disclosure?

Division of Corporation Finance
Securities and Exchange Commission

CF Disclosure Guidance: Topic No. 2

Cybersecurity

Date: October 13, 2011

Summary: This guidance provides the Division of Corporation Finance's views regarding disclosure obligations relating to cybersecurity risks and cyber incidents.

D&O Insurance?

Cybersecurity Insurance?

Target's Cyber Insurance Softens Blow of Massive Credit Breach

By Dhanya Skariachan and Jim Finkle | February 26, 2014

Advising the Board During a Breach

- **Board must gain understanding of the scope of the breach and the business and legal implications of the breach.**
- **Board involvement:**
  - Board members must become informed.
  - Consider using a committee for daily or more regular communication (refer to incident response plan).
  - Consider having third-party engaged in the investigation or remediation speak directly to the board or Risk Committee.
  - Oversee management's decisions and responses.
    - May include receiving reports on the action plan such as response times, appointment of "breach czar," and action plan testing, as well as reports on containment and remediation plans.

Questions?

Follow us: @AlstonPrivacy
www.AlstonPrivacy.com