Director and Officer Liability & Cyber-Security

4 Questions Every Officer and Director Must Answer

Richik Sarkar, Member
McGlinchey Stafford

Frances Floriano Goins, Partner
Ulmer & Berne LLP

September 9, 2016

McGLINCHEY STAFFORD
www.mcglinchey.com

Ulmer
ulmer.com

Director and Officer Personal Liability for Cyber-Breaches

- In line with controlling state statutes, courts historically have set a high threshold to find directors and officers personally liable for breaches of fiduciary duties
- However, the standard for director oversight liability is evolving because of high stakes and increased publicity from cyber-breaches

What are Directors' Fiduciary Duties with Respect to Cyber-security?

Business Judgment Rule

- A rebuttable presumption that directors will not be second-guessed when they act on an informed basis, in good faith, and in honest belief that action was in the best interests of the company (applies only when directors "act")
- Failure to exercise appropriate oversight may impose personal liability on directors for losses caused by non-compliance with legal standards
  - *In re Caremark International, Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996)
- At a minimum, when directors have actual knowledge of facts that should put them on notice of illegal or improper conduct, they must take good faith steps to remedy the problem, including measures to prevent recurrence and to stop the problem from materializing or progressing
  - *Stone v. Ritter*, 911 A.2d 362 (Del. 2006)
- Officers may be judged by a different standard, depending on state law and/or employment contract

Cyber-Security Issues

- Courts will specifically analyze how boards are identifying, assessing, and addressing cyber risk
- Proper board preparedness and planning are critical to insulating officers and directors from liability

Palkon v. Holmes

- Shareholder action against directors, president/CEO, and general counsel of Wyndham Worldwide Corp.
- Suit followed three data breaches between April 2008 and January 2010; breaches resulted in the theft of over 600,000 customers' credit card information
- Allegations of breaches of fiduciary duties of care and loyalty, and waste of corporate assets
- Case was dismissed

Palkon v. Holmes cont.

- Business Judgment Rule protected the board because the board:
  - Held 14 quarterly meetings discussing the cyber-attacks, company security policies, and proposed security enhancements
  - Charged audit committee with oversight of response to breach; audit committee met multiple times to review cyber-security and investigate the breaches
  - Hired a technology firm to recommend security enhancements, which the company had begun to implement
  - Had cyber-security measures in place that had been discussed many times by the board prior to the breach

Cautionary Tale of *In re: Lemington Home for the Aged*

- Appellate court upheld jury finding of personal liability for non-profit directors' breach of fiduciary duty
- Directors found not to have exercised reasonable care
  - Allowed underperforming and unqualified officers to remain in their roles and failed to remove them when results of their mismanagement were made clear
- Court ultimately found directors liable for "willful blindness" mismanagement

What Does This Mean?

- *Palkon* established a framework for actions officers and directors can take to protect themselves and their organizations from liability
- *In re: Lemington Home for the Aged* showed what can happen if proper cyber-risk management and protocols are not put in place and consistently monitored by management and the board

Director and Officer Liability

- In the context of cyber-security, liability is determined not only by how potential problems are anticipated and addressed, but how the board responds when actual issues arise
- Boards have a duty to investigate when issues arise and should begin as soon as possible after a triggering event
- Taking steps to correct underlying issues after an incident will help deflect liability

Independent, Outside Counsel Should Conduct Investigation

- Although in-house legal or compliance departments may be capable of conducting the investigation, boards should utilize outside counsel because:
  - use of outside counsel can cement attorney-client privilege, protecting critical and confidential information and analysis from discovery
  - engaging outside counsel with other advisors can help support invocation of the Business Judgment Rule

How Can Officers and Directors Properly Discharge Their Cyber-Security Fiduciary Duties?

NIST

- The National Institute of Standards and Technology (NIST) Cyber-security Framework created a template that corporations, directors, and officers can adapt to their organizational needs

SEC

- The Securities and Exchange Commission (SEC) has provided guidance for boards seeking to comply with their oversight and disclosure obligations in the cybersecurity arena as a part of enterprise risk management
- The SEC issued CF Disclosure Guidance: Topic No. 2 on October 13, 2011, providing insight on disclosure obligations related to cybersecurity risks and cyber incidents

Proper Discharge of Fiduciary Duties

- Directors and officers must be aware of applicable laws and industry standards related to cybersecurity and data privacy and understand how their organizations:
  - Hold data, and what data is mission critical
  - Identify risks and potential areas of weakness
  - Protect against cyber-attacks
  - Detect triggering events and cyber-breaches
  - Transfer financial responsibility after a cyber-event occurs
  - Respond to cyber-breaches
  - Recover from cyber-security events

Hallmarks of Truly Effective Cyber-Risk Governance

- Strategies should include:
  - Defined roles for directors and management
  - Constant re-assessment of cyber-security trends and threats
  - Cyber-security vigilance permeating the organization through appropriate training
  - Continually evolving cyber preparedness plans and controls
  - Detailed incident response protocols
  - Comprehensive insurance coverage
  - Educating themselves on technology and data security issues
  - Ensuring the entity has a comprehensive vendor management program
  - Considering opportunities for cybersecurity information sharing

What is the Potential Exposure for Directors and Officers as the Result of a Cyber-Incident?

Potential Exposure From Consumer Lawsuits

- Traditionally, courts require a showing of actual harm to support Article III standing to sue in federal court
- The Seventh Circuit Court of Appeals granted Article III standing to a class of persons whose personal data had been compromised without this showing because there was an "objectively reasonable likelihood" that an injury would occur due to a cyber-security breach
  - *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015)

What Does This Mean?

- The holding in *Remijas* arguably reduced a barrier for consumer data-breach lawsuits and will likely result in an increase of actions

Recent Cases

- *Spokeo v. Robins*, 136 S. Ct. 1540 (2016)
  - Plaintiffs must allege a concrete injury to obtain Article III standing
  - Alleging violation of statute does not automatically confer standing
- *Khan v. Children's National Health System*, No. TDC-15-2125, 2016 WL 2946165 (D. Md. May 19, 2016)
  - Court held that absent specific incidents of misuse of stolen data, increased risk of identity theft does not meet concrete injury requirements

Potential Exposure from Shareholder Derivative Lawsuits

- It has become common for shareholder derivative lawsuits to follow disclosure of a substantial data breach
- “Harm” will be damage to the company’s finances and reputation

How Can Officers and Directors Reduce Their Risks?

Shifting the Focus

- The focus must be shifted from questions of liability and defense to questions of offensive and proactive stewardship
- Companies, at the direction of the board, should:
  - Deliberately and consistently educate directors about industry best practices and the company's cyber-security policies, controls, and procedures
  - Create cross-disciplinary, broad-based cybersecurity committees or groups to be primarily responsible for data privacy and other cyber-security issues
  - Create ongoing training programs for employees to educate everyone about their cybersecurity responsibilities
  - Create a detailed incident response plan
  - Conduct regular reviews of cybersecurity to ensure that the company's expectations and procedures are being diligently followed

Recent Derivative Actions Relating To Cyber-Security

TARGET

Target

- Fell victim to cyber-attack in 2013
- Shareholders filed suit against Target's board and executive management alleging:
  - Failure to properly provide for and oversee an effective information security program
  - Failure to give customers and the public prompt and accurate information in disclosing the breach
- The Special Litigation Committee (SLC) that was formed to investigate those allegations concluded that pursuing the claims was not in Target's best interests. Following the SLC's recommendation, the Court dismissed the action.


THE
HOME
DEPOT
®

Home Depot

- Fell victim to one of the largest data breaches in U.S. history in 2014
- Shareholders filed a derivative suit against Home Depot and its directors and officers in August 2015 alleging:
  - Breach of fiduciary duties by failing to ensure company took reasonable steps to protect consumers' personal and financial information
- Litigation currently ongoing

Wendy's

McGLINCHEY STAFFORD
www.mcglinchey.com

Ulmer
ulmer.com

Wendy's

- Wendy's fell victim to a series of cyber-attacks beginning in October of last year
- Hackers were able to obtain cardholder names, credit or debit card numbers, and expiration dates
- There has been no derivative litigation to date, but a law firm is investigating the matter on behalf of the shareholders
- Two class action suits (consumer and card-issuing banks) have been brought
  - Consumer action was dismissed for lack of standing

What's on the Horizon?

Federal Cybersecurity Initiatives

- Cybersecurity Information Sharing Act of 2015
  - Intended to encourage companies to share cyber-threat information with the Federal government (through Department of Homeland Security), local governments, and private entities
  - Includes an antitrust exemption
  - Protection from liability for information sharing and monitoring information
- President Obama's Cybersecurity National Action Plan, which includes:
  - Establishing a Commission on Enhancing National Cybersecurity
  - Strengthening federal cybersecurity
  - Empowering individuals to secure consumer data

Senate Bill 2410

- Cybersecurity Disclosure Act of 2015 (does not have a high chance of passing)
- Would require companies to:
  - Disclose whether any directors or officers have expertise or experience in cybersecurity, with details about that experience or expertise; and
  - If no director or officer has expertise or experience, describe the cybersecurity steps taken in identifying and evaluating nominees for directors and officers

Richik Sarkar
(216) 378-4994
rsarkar@mcglinchey.com
McGlinchey Stafford
25550 Chagrin Blvd.
Suite 406
Cleveland, OH 44122-4640

Frances Floriano Goins
(216) 583-7202
fgoins@ulmer.com
Ulmer & Berne LLP
1660 West 2nd Street
Suite 1100
Cleveland, OH 44113-1448