# Mastering Online Surveillance, GDPR, & Cyber Security Law

Rossdale CLE

March 1, 2018

Melissa Krasnow, VLP Law Group LLP, Minneapolis

Email: mkrasnow@vlplawgroup.com

Attorney biography:

http://www.vlplawgroup.com/attorneys/melissa-krasnow/

SLIDES

STATE BREACH NOTIFICATION AND STATE DATA SECURITY LAWS

INCIDENT RESPONSE PLANS AND TABLETOP EXERCISES (TTX)

CYBER LIABILITY INSURANCE

ADVISING THE BOARD

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

ADDITIONAL RESOURCES

# STATE BREACH NOTIFICATION AND STATE DATA SECURITY LAWS

48 states, plus the District of Columbia, Guam, Puerto Rico and Virgin Islands, have breach notification laws that require notification of a breach to affected individuals

16* of the states with breach notification laws also have laws addressing security procedures

Stay tuned for developments

*Delaware's amendment to its law becomes effective April 14, 2018

## STATE BREACH NOTIFICATION AND STATE DATA SECURITY LAWS (Con't)

Personal information is generally defined by state breach notification and state data security laws as name, plus any of:

- Social security number
- driver's license number or other government-issued identification number
- credit or debit card or account information with or without password
- medical information
- health insurance information
- biometric information
- DNA profile or
- online account information

# STATE BREACH NOTIFICATION AND STATE DATA SECURITY LAWS (Con't)

27* state laws, plus Puerto Rico law, also require notification of a breach to a state attorney general or regulator in addition to the affected individuals

5* state laws cover identity theft prevention and mitigation services

Has identity theft prevention and mitigation service provider been engaged?

*Delaware's amendment to its law becomes effective April 14, 2018

# STATE BREACH NOTIFICATION AND STATE DATA SECURITY LAWS (Con't)

A written information security program may be required by certain state data security laws

For additional information, please see:

https://www.vlplawgroup.com/blog/vlp-partner-melissa-krasnow-co-authors-two-resources-thomson-reuters-practical-law-written-information-security-programs-compliance-massachusetts-data-security-regulation-2/

Will there be a comprehensive federal breach notification and data security law?

# INCIDENT RESPONSE PLANS AND TABLETOP EXERCISES (TTX)

Is there an incident response plan and / or business continuity / disaster recovery plan?

When was the last time each was tested or updated?

How frequently is each tested or updated?

What was the situation that was the subject of the testing?

What are the results of and insights from testing or updating?

Who are the members of the incident response team?

Who are external team members, including service providers?

What are incident response team member responsibilities?

# INCIDENT RESPONSE PLANS AND TABLETOP EXERCISES (TTX) (Con’t)

Is there contact information for incident response team members?

What are the lines of communication?

What communications/disclosures/notifications are anticipated (e.g., internal and external)?

Prepared to work with law enforcement, regulators, industry contacts and business partners?

Is any training or awareness provided for employees, etc.?

# CYBER LIABILITY INSURANCE

Cyber liability insurance policy has the following basic coverages:

Third Party
1. Security and privacy legal liability
2. Regulatory liability
3. Payment Card Industry (PCI) liability
4. Media liability

First Party
1. Beach response expense
2. Business interruption
3. Data asset recovery
4. Extortion

Source: Steve Krusko, Chief Underwriting Officer, Berkley Cyber Risk Solutions, a W.R. Berkley Company

## CYBER LIABILITY INSURANCE (Con't)

Emerging coverage grants available by endorsement or within certain updated policy forms:

1. Social engineering crime loss
2. Computer crime
3. Systems failure extension for contingent/dependent business
4. Reputation loss
5. Wrongful collection
6. Affirmative grants for bodily injury or property damage resulting from a cyber event
7. Affirmative grants for General Data Protection Regulation (GDPR)
8. Integrated cyber policies
9. Expanded regulatory coverage

Source: Steve Krusko, Chief Underwriting Officer, Berkley Cyber Risk Solutions, a W.R. Berkley Company

# ADVISING THE BOARD

## Wyndham Shareholder Derivative Lawsuit Dismissed (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)

## ADVISING THE BOARD (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

## ADVISING THE BOARD (Con’t)

## Home Depot Shareholder Derivative Lawsuit Settlement (Delaware law)

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

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

## ADVISING THE BOARD (Con’t)

## Home Depot Shareholder Derivative Lawsuit Settlement (Delaware law)

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

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)

## ADVISING THE BOARD (Con't)

## Home Depot Shareholder Derivative Lawsuit Settlement (Delaware law)

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)

Please see:

Director Liability: Boards are on the hot seat over data breaches, illegal sales practices and more.

https://www.directorsandboards.com/articles/singledirector-liability-boards-are-hot-seat-over-data-breaches-illegal-sales-practices-and

## ADVISING THE BOARD (Con’t)

## Target Shareholder Derivative Lawsuit Dismissed (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)

# ADVISING THE BOARD (Con’t)

## Equifax Shareholder Derivative Lawsuit (Georgia law)

Assad v. Smith, No. 1:18-cv-00477-TWT (N.D. Ga.)

# ADVISING THE BOARD (Con’t)

Securities Class Action Lawsuits Involving Directors & Officers

Please see:

More Companies Face Securities Fraud Suits After Data Breaches

https://www.bna.com/companies-face-securities-n57982088684/

# ADVISING THE BOARD (Con't)

Securities and Exchange Commission Statement and Guidance on Public Company Cybersecurity Disclosures

A company must include a description of how the board administers its risk oversight function. To the extent cybersecurity risks are material to a company's business, we believe this discussion should include the nature of the board's role in overseeing the management of that risk.

In addition, we believe disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area.

Source: https://www.sec.gov/rules/interp/2018/33-10459.pdf

## 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

# ADDITIONAL RESOURCES

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

https://www.irmi.com/biographies/melissa-krasnow