March 2015 • Vol. XXVIII • Number 3

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

Kenneth Labbate *is a partner with the firm Mound Cotton Wollan & Greengrass. He has over 20 years' experience in defending complex civil litigations on behalf of accountants, attorneys, insurance agents and brokers, architects, engineers, real estate brokers, and other miscellaneous professionals. He can be reached at klabbate@moundcotton.com.*

Oliver Twadell *is an associate with the law firm of Mound Cotton Wollan & Greengrass, where he works on a range of litigation defense matters, including cases involving complex property damage issues, contract disputes, labor law, and other issues. He can be reached at otwaddell@moundcotton.com.*

Corporate Risk Presented by Ever Evolving and Growing Cyber Crime: Trying Times for Directors & Officers

By Kenneth M. Labbate and Oliver E. Twaddell

In late 2013, Target was reeling from a massive data breach. Now, just before the December holidays, Sony is dealing with its second significant data breach. Sony's initial breach resulted in the theft of personally identifiable information for more than 80 million of its customers. This time it appears from initial reports that not only was personally identifiable information stolen again, but in addition, certain proprietary information was also stolen from Sony Pictures Entertainment Inc., a subsidiary of Sony Corp., in the form of a film set for release and a screenplay, raising the specter of potential legal exposure for both the company and its directors and officers.[1]

Although there are many areas of exposure for businesses that lose important and classified information, one of the most potentially significant and least developed has been the liability of the directors and officers of these companies. The consensus is, however, that claims in this area will not be the exception for much longer, particularly as the frequency of data breaches grows.[2,3] What distinguishes the recent breach at Sony Pictures from the earlier breach and most significant breaches which have been reported is the theft of intellectual property from Sony Pictures. How does the theft of essential pieces of business affect not only shareholder equity, but potentially a company's viability? How can companies prevent or mitigate potential exposure, particularly in light of the ever-increasing prominence and sophistication of the "hack-tivist"? What is the duty of today's directors and officers to protect against such losses and mitigate exposure if and when data breaches occur? How do today's directors and officers satisfy their fiduciary obligations by keeping up with the ever-changing and evolving "cyber-criminal"?

This article will explore what directors and officers should be doing now to protect the interests of corporate shareholders and minimize their own exposure to liability.

* * *

According to the Ponemon Institute's 2014 report, the average cost of a data breach in the United States is $5.9 million per incident and $201 per individual record.[4] These costs make up only a small portion of the pie. Data breaches in which personal data is stolen can cause customer, client, employee and investor dissatisfaction, resulting in a loss of trust and reputational harm. However, the effect of these past breaches does not seem, as of yet, to be negatively affecting a company's stock price. Whether and to what extent the theft of proprietary information alters a company's stock price is yet to be seen.

As these risks are not always preventable, what should directors and officers do to prevent such data breaches, and how should they react to such events? As will be explained, there are numerous safeguards that can be implemented to protect the company and its shareholders from a diminution in value as well as the directors and officers from liability.

As an initial matter, it should be kept in mind that the well-established business judgment rule continues to govern a director's duty of care in making business and managerial decisions. The rule presumes that when a director makes a business decision, it is made "on an informed basis, in good faith and in the honest belief that the action is in the best interests of the company." *Smith v. Van Gorkom*, 488 A.2d 858 (Del. 1985). In evaluating due care, courts will "look for evidence of whether a board has acted in a deliberate and knowledgeable way identifying and exploring alternatives." *Citron v. Fairchild Camera and Instrument Corp.*, 569 A.2d 53 (Del. 1989). Even though directors may rely on reports prepared by others, they may not rely solely on retained experts and management without taking an active and direct role. Thus, the board of directors that neglects to actively monitor and manage its company's cyber-security will undoubtedly face heavy scrutiny.[5]

Data breach cases have not yet provided much insight into the due diligence expected of directors and officers to determine whether they have satisfied their duty of care. Recently, however, an otherwise unremarkable decision provided some guidance on this question. In *Palkon ex rel. Wyndham Worldwide Corp. v. Holmes*, the hospitality company Wyndham Worldwide Corporation was sued by Dennis Palkon, one of the corporation's shareholders, after it refused Palkon's demand to bring a lawsuit on behalf of the corporation relating to the failure of the directors to familiarize themselves with the data breach. From April 2008 to January 2010, Wyndham had been the victim of three separate data breaches that resulted in the theft of credit card and personal information of over 600,000 customers. Soon after the breaches, the FTC brought an action against Wyndham, challenging its data security practices (the "FTC Action"). In a separate derivative action, plaintiff Palkon alleged that Wyndham and numerous of its corporate officers "failed to implement adequate data-security mechanisms, such as firewalls and elaborate passwords, and that this failure allowed hackers to steal customers' data." Palkon further alleged that the defendants "failed to timely disclose the data breaches after they occurred."[6]

In granting defendants' motion to dismiss, the U.S. District Court in New Jersey found that Wyndham's board of directors had taken various steps to familiarize itself with the data breach. Specifically, the board had undertaken a number of actions to conduct a "reasonable investigation" into the data breach, including:

(a) the board discussed the cyber-attacks at fourteen meetings from October 2008 to August 2012, and gave a presentation about the breaches and Wyndham's data security and proposed security enhancements;

(b) the board discussed with the audit committee the same data breach and security issues in at least sixteen committee meetings during the same time period;

(c) the board hired technology firms to investigate each breach and to issue recommendations on enhancing the company's security; and

(d) after the initial breaches, the board began to implement the recommendations.[7]

Also important to the court's assessment of the board's activity was that the board had developed information about the breaches through the FTC Action that Wyndham was facing. The court was influenced by the board's time and interest in discussing the data breaches, becoming fully knowledgeable about the issues concerning Palkon's later demand letter, and implementing certain recommendations made by the retained technology firms.

The *Palkon* decision offered some insight into what a board should consider when faced with a data security breach, when responding to and investigating the breach, and in trying to prevent future breaches. As illustrated by the *Palkon* decision, directors and officers must take certain steps in order to prevent or minimize the effect of data breaches, and provide a foundation from which to defend against allegations of breach of fiduciary duty. What remains clear is that when a data breach occurs (and it likely will), plaintiffs' lawyers will look to scrutinize the decisions made by directors and officers in allocating resources to assess and investigate the risk of a breach and to detect and respond to a breach in a timely and effective manner. While achieving this balance is made difficult by the increasing and rapidly evolving risks presented by the cyber-criminal, there are a number of actions that directors and officers can take and questions they can ask to protect themselves and the companies they serve from liability: [8]

- Develop a clear understanding of the company's cyber-security processes and procedures in order to be certain that the company is sufficiently protected in this constantly evolving technology world;
- Hire a reputable security software provider;
- Conduct periodic and frequent tests of the company's cyber-security protocols and safeguards and have consistent and frequent communications regarding the company's cyber-security guidelines for dealing with a data breach;
- Appoint a chief information security officer with expertise on cyber-security and data breaches. Require this officer to regularly update the board on proper protocol and recommend changes when needed. The CISO's premier responsibility should be to vigilantly stay attuned to the company's information security and regularly advise the board regarding the same;
- Form a cyber-security committee responsible for privacy and security that meets regularly and keeps the board abreast of the company's cyber-security efforts and issues, making timely recommendations for the detection and prevention of data breaches. The cyber-committee should consist of individuals from executive management, information technology, legal, risk management, public relations, and the audit and compliance departments;
- Ensure that the company encrypts data transfers;[9]
- Become knowledgeable on applicable privacy and data breach disclosure laws. Senior management should identify all sensitive data, including personal information, healthcare information, and customer financial and identifying information, and implement safeguards and controls to protect that sensitive information;
- Understand outside vendors' cyber-security protections, and make sure that vendors that have access to company systems and information have sufficient safeguards and recovery plans. As seen in the Target and Home Depot data breaches, the company was infiltrated by the flawed cyber-security protection of outside vendors;[10]
- Make certain cyber-security measures of vendors with which the company does business meet the company's own standards. Utilize indemnification and additional insured provisions to shift risk (and cost) of data breaches to vendors and to minimize the company's exposure to vendor related breaches;
- Adopt and test a data breach response plan that complies with the laws of the individual states your company is doing business in;
- Ensure that any breach response plan provides for proper notice of a cyber-incident to insurers for all possible insurance lines of coverage. The response plan should also account for how the company will respond to various actors in the aftermath of a data breach, *e.g.*, the media, law enforcement, customers, clients and vendors;
- Periodically use an outside company to audit the company's cyber-security protocol, and compare those findings to the steps and processes recommended by the company's cyber-officers and cyber-committee;
- Ensure that the company has formal written cyber-security practices and procedures with regard to any sensitive data held by the company. The cyber-

security officers and committee should periodically review and update these written rules and procedures. The board should be fully knowledgeable about these written procedures, and should oversee any drafting and revisions to these standard procedures;

- Review the company's cyber-insurance, directors' and officers' commercial general liability, and any other potentially applicable coverages, to be certain the company is adequately protected;[11]

- Identify and quantify any cyber-exposures, and mitigate those exposures, including conducting due diligence, reviewing contractual allocation of liability and implementing information technology best practices in accordance with the National Institute of Standards and Technology Critical Infrastructure framework. This cyber-security guideline is likely to become the security requirement for data breach litigation;[12]

- Mandate periodic training and education sessions for all employees about cyber-risks;

- Comply with the Security and Exchange Commission's disclosure guidance on cyber-security, including potentially disclosing: cyber-security risk factors that arise from the company's business or operations, any of the company's outsourced functions that create cyber-liability risks, material cyber-incidents experienced by the company and their costs and consequences, and a description of the company's relevant insurance coverage.[13]

In this relatively new age of data breach liability, individual plaintiffs have had difficulty in proving compensable damages.[14] Without any proof of misuse of their personal information or bank card, establishing a *present*, non-speculative harm is difficult.[15] But as we have seen in the Target litigation, financial institution plaintiffs have alleged a number of damages: the capital and human resources needed to address the breach, including reissuing cards, changing or closing accounts, notifying customers of the breach of their cards, investigating claims of fraudulent activity, refunding customers for fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and lost interest and transaction fees as a result of decreased or ceased card usage.[16]

The damages alleged by financial institution plaintiffs seem rather obvious, but the more problematic question for plaintiffs' lawyers has been: what damages does an individual shareholder or a class of shareholders suffer when their credit card or personal information is stolen? The recent major data breaches, *e.g.*, Target and Home Depot, did not result in more than a nominal change in the company stock prices.[17] It remains unclear what the impact of the theft of proprietary information or intellectual property will be, but the potential effect on a company's stock price is clear. Implementing many of the above recommendations will provide the foundation from which a defense can be built on behalf of a director or officer who is accused of neglect in analyzing the risk of, and in responding to, a data breach.

* * *

The novel cyber-risks now faced by companies, both large and small, place businesses in a difficult position to make well-informed monetary decisions about how to most effectively allocate company resources. As data breaches continue to occur, plaintiffs will continue to develop damages theories which will become increasingly easier as the cyber-criminal focus shifts from the theft of personally identifiable information to the theft of proprietary information and intellectual property, as was recently reported at Sony Pictures.

It is up to a company's directors and officers to ensure that resources are properly and timely allocated to assess and respond to the cyber-risks a company faces so as to protect and preserve a corporation's intellectual property and correspondingly, shareholder equity. The failure of a director or officer to properly discharge his or her duty in this regard will continue to be an ever increasing focus in the data breach world.

Endnotes

1 Sony Pictures Entertainment Inc. is the subject of a Class Action proceeding in the United States District Court – Central District of California filed by current and former employees of the company.

2 *See* Prepared Remarks of Robert Mueller, Cyber Security Conference (Mar. 1, 2012).

3 Cyber-related directors and officers liability claims expected to increase, Management Liability, Nov. 10, 2014.

4 Ponemon Institute, *2014 Cost of Data Breach Study: United States*, May 2014.

5 D. Barres and D. Picca, Corporate Counsel, "Director Liability for Cybersecurity Risks," Aug. 6, 2014.

6 *Palkon ex rel. Wyndham Worldwide Corp. v. Holmes,* 2014 WL 5341880 (DN.J. Oct. 20, 2014).

7 *Id.*

8 *See* L.J. Trautman and K. Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, The John Marshall Journal of Computer & Information Law, Volume XXVIII, 3, 2011.

9 *See* L. Unger, *Breaches to Customer Account Data*, Journal of the Missouri Bar, Sept.-Oct. 2014.

10 *See* K. LaCroix, *Guest Post: The Cloud, Cyber Security and Cloud Cyber Governance: What Every Director Needs to Know,* The D&O Diary, July 29, 2014.

11 A. Radke and J. Cleary, Lessons from Dismissal of Wyndham Shareholder's Derivative Action, Nov. 19, 2014.

12 K. Kalinich and M. Becker, Cyber Risk: Are Boards the New 'Target'?, April 22, 2014.

13 On October 13, 2011, the SEC, Division of Corporation Finance, released cyber-security disclosure guidance entitled "CF Disclosure Guidance: Topic No. 2 – Cybersecurity." As made clear by the guidance, it is not a rule, regulation, or statement of the SEC. However, it may be important to disclose this information, depending on the company's particular facts and circumstances. For example, plaintiffs in shareholder litigation will challenge non-disclosures or inadequate disclosures of important cyber-security risks in order to buttress claims against the company and its directors and/or officers. The SEC's guidance can be found at: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

14 D. Meal, *Privacy and Surveillance Legal Issues*, 2014.

15 *See, e.g., Pisciotta v. Old Nat. Bancorp,* 499 F.3d 629 (7th Cir. 2007).

16 Consolidated class action complaint against Target, August 1, 2014, filed in the U.S. District Court for the District Court of Minnesota; MDL No. 14-2522. *See also Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc.,* 729 F.3d 421 (5th Cir. 2013).

17 Compare *Heartland Payment Systems, Inc. Securities Litigation,* 2009 WL 4798148 (D.N.J. December 7, 2009). Heartland Payment Systems was sued in a securities fraud class action when its system was breached, resulting in the theft of millions of credit and debit card numbers. The breach occurred over the course of 2008, and was not discovered by Heartland until 2009. At that point when Heartland disclosed the breach, its stock price dropped 80 percent. However, the shareholder class action was dismissed because they failed to plead fraud with particularity as required under the Private Securities Litigation Reform Act of 1995. The officers and directors, however, did settle with Visa, MasterCard, and American Express.