# DIRECTORS AND OFFICERS: BE WARY OF GROWING CYBER RESPONSIBILITIES

**By Jonathan E. Meer** - First published: BLD Bach Langheid Dallmayr Financial Lines Newsletter November 2018

The increased reliance of businesses on the Internet has led to faster communication and greater efficiency, but such reliance comes with possible tales of woe when technology fails or is misused. Directors and officers (D&Os) are often the ones who put the final stamp of approval on such things, and there is a growing trend to hold those same people personally liable when there is a turn for the worse. Cyber exposure for businesses has only increased in the past couple of years and the laws and regulations are starting to catch up. This exposure has been in the form of data breaches and the subsequent data restoration and notification costs, as well as in lawsuits and government regulations. Recent lawsuits targeting D&Os for their alleged failure to address cyber risk provide examples of potential liability as more regulations are passed in the United States and around the world. D&Os should be aware of the informal and formal standards that are being set regarding appropriate company cyber risk management.

## Lawsuits against D&Os in the United States Related to Cyber Risk

Private actions aimed to hold D&Os accountable for cyber risk in the United States is nothing new. Securities class action lawsuits, such as those against Wyndham, Heartland Payment, and Target were brought alleging breach of fiduciary duty with respect to handling a cyber breach.[1] Specifically, the allegations in these litigations against the D&Os were for failing to (1) implement and enforce effective internal controls with respect to data security, (2) disclose the effectiveness of a company's data security policies, (3) disclose the scope of the data breach, and (4) exercise oversight duties on how a security breach could adversely affect the company's business. These claims often focus on alleged breach of duty when there is a failure to adequately implement cyber security defense in the first place, or involve failing to respond to and otherwise monitor cyber security plans after a breach has occurred. What all these referenced cases also have in common is that they were defended and dismissed without any liability to the D&Os.

The success of the D&Os' defenses in these matters has neither deterred more lawsuits from being filed in the United States nor stopped D&Os from settling cases alleging breach of fiduciary duty in connection with cyber risk. The D&Os of Home Depot were successful in defending such a claim, but chose to settle the matter when the dismissal was appealed.[2] The D&Os of Wendy's, while their motion to dismiss was pending, also chose to settle.[3] It remains to be seen how the D&Os of Yahoo, Equifax, and Google will respond to the pending claims against them for alleged cyber security failures.[4]

---

1 *Wyndham - Dennis Palkon, et al. v. Stephen P. Holmes, et al.* **14-cv-01234, (U.S. District Court for the District of New Jersey)**; *In re Heartland Payment Systems, Inc.*, 09-CV-01043 (U.S. District Court for the District of New Jersey); Target - *Mary Davis et al. v. Gregg W. Steinhafel et al.*, **14-cv-00203, (U.S. District Court for the District of Minnesota)**.

2 *In Re The Home Depot, Inc. Shareholder Derivative Litigation,* **15-CV-2999 (U.S. District Court for the Northern District of Georgia)**.

3 *Graham, et al. v. Nelson Peltz, et al.,* **16-cv-1153, (U.S. District Court for the Southern District of Ohio)**.

4 *Madrack v. Yahoo! Inc., Marissa Mayer, et al.,* **17-cv-0037 (U.S. District Court for the Northern District of California)**; *Kuhns v. Equifax, Inc., et al.,* **17-cv-3463, (U.S. District Court for the Northern District of Georgia)**; *Mawardy v. Alphabet, Inc., et al.* **18-cv-5704 (U.S. District Court for the Eastern District of New York)**.

## Regulations Impacting Corporate Cyber Risk

Coupled with these recent litigations are new government regulations to which D&Os must respond in connection with corporate responsibility and disclosure on cyber risk. While the General Data Protection Regulation (GDPR) has gotten most of the headlines, there have been other regulations in the United States and Canada that are impacting D&Os.

The GDPR, effective May 2018, has been a big topic of discussion because it addresses, amongst other things, information collected and data breach responsibilities. Per a recent 2018 Advisen Ltd. survey, nearly 40% of large companies, defined as over $1 billion in revenue, have made changes with respect to cyber issues as a result of the GDPR. As the GDPR focuses on the control, processing, and use of the data and information of European Union citizens, D&Os are the ones responsible for implementing the corporate governance framework. Article 5(2) of the GDPR specifically reads that the "controller shall be responsible for, and be able to demonstrate compliance with, [the other data protection principles]." Article 24 describes in greater detail the responsibility of the controller, which includes implementing "appropriate technical and organizational measures to ensure and to be able to demonstrate the processing is performed in accordance with this regulation." The regulation also requires under Article 37 that certain businesses designate a data protection officer who must report to the highest level of management, operate independently, and have adequate resources to carry out their tasks. Since the GDPR has been in effect only for a couple of months, it remains to be seen how it will be enforced.

Another recent cyber regulation is promulgated by the New York State Department of Financial Services (NYSDFS) for those companies subject to its jurisdiction. Under 23 NYCRR Part 500, effective in March 2017, New York provided clear notice that it intends to hold directors and officers more responsible for ensuring that their companies are undertaking more active assessment of their own security policies and procedures. These include the enactment of a comprehensive cybersecurity policy, a written incident response plan that reports breaches within 72 hours to the NYSDFS, and security policies for third-party service providers who access nonpublic information. The new rules also put more responsibilities on directors and officers, requiring not only the designation of a chief information security officer (CISO) but also board certification to the NYSDFS of compliance with the regulations. As of September 3, 2018, regulated entities are required to (1) maintain financial and cyber audit trails; (2) maintain written procedures for evaluating, assessing, or testing cybersecurity; (3) maintain policies and procedures on secure disposal on a periodic basis of nonpublic information no longer necessary for business operations; (4) have a training program to monitor activity of authorized users; and (5) have encryption controls to protect nonpublic information held. By March 1, 2019, the transition period under the NYSDFS regulation will be over and compliance with the full cyber regulation will be required.

Another regulation in the United States that will be coming into effect soon is the California Consumer Privacy Act (CaCPA), which was passed on June 28, 2018, and will be effective January 1, 2020, with enforcement by July 1, 2020. Businesses that collect or sell personal information either from or about California consumers must comply with the CaCPA. The regulated businesses subject to the CaCPA also must (1) have annual gross revenue of $25 million; (2) collect personal information of at least 50,000 consumers, households, or devises; or (3) obtains at least 50 percent of annual revenue from selling consumers' personal information. Similar to the GDPR, the CaCPA was designed to give California residents control over the use, including the sale, of their personal information. One key aspect of the CaCPA is that a business cannot provide a different level or quality of services based on a consumer objecting to their sale of the data, except where it is "reasonably related to the value provided to the consumer by the consumer's data." Since the CaCPA will not be in effect until 2020, there will likely be some further clarifications to its regulations.

The most recent cyber protection law, the Personal Information Protection and Electronic Documents Act (PIPEDA), effective November 1, 2018, is a Canadian law that applies to the collection, use, and disclosure of personal information in the course of commercial activities in all of Canada. Foreign and domestic organizations subject to PIPEDA will be required to (1) notify individuals about privacy breaches when there is "a real risk of significant harm to an individual," (2) keep records of such breaches, and (3) report cyber breaches to the Canadian government. Failure to comply can lead to fines up to CAD$100,000. While this potential fine is far less than that levied by the GDPR, the regulation still has some teeth.

The regulations in the EU, Canada, New York, and, soon California stress to D&Os the importance that governments are putting on cyber security.

## Takeaways

While the advantages of the Internet usually outweigh the potential liabilities, D&Os need to be aware of the risks posed by cyber exposure. It is important to implement written policies and procedures and training that (1) provide guidance to officers and employees concerning applicable threats and measures to prevent, detect, and respond to such threats, and (2) monitor compliance with cybersecurity policies and procedures.

The risks are not limited to a company's computers; they also exist in the company's use of wearables and products connected to the Internet of Things. Exposure to cyber security threats exists everywhere, so what is disclosed to shareholders and the public by D&Os about such risks takes on heightened importance. The cyber risks are growing by the day, and with them, potential liability for D&Os. Being aware of the changing standards of care and rules and regulations is an essential first step for D&Os in their challenge to serve the best interests of their respective companies.

---

— By **Jonathan E. Meer**, Wilson Elser Moskowitz Edelman & Dicker LLP

**Jonathan E. Meer**: Jonathan has successfully participated in mediation and litigation of D&O and other insurance coverage disputes. He regularly represents D&O insurers as coverage and monitoring counsel in complex shareholder class actions against public companies and their directors and officers for violations of federal securities laws and in shareholder derivative suits against directors and officers for breach of fiduciary duty and mismanagement in the context of mergers and acquisitions and other business transactions. Jonathan can be reached at 212.915.5639 or jonathan.meer@wilsonelser.com.