ulmer | berne | llp
ATTORNEYS

FRANCES FLORIANO GOINS
Partner
direct 216.583.7202
direct fax 216.583.7203
fgoins@ulmer.com

Addressing Cybersecurity Risk in the Board Room

As the pace and extent of data breaches of U.S. companies continues to accelerate, corporate directors have become more aware of the attendant risks not only for their companies, but for themselves. Unfortunately, however, despite the escalating costs associated with such incidents,[1] this increased attention has not uniformly translated into appropriate risk management policies and procedures. Regulators have taken notice of the disparity, and cybersecurity has become a priority of both the Securities and Exchange Commission (SEC) and the Department of Homeland Security (DHS).

According to a recent release by EisnerAmper LLP reporting on a survey of responses from directors of more than 250 boards, reputational risk and cybersecurity are the two major concerns (aside from financial risk) of directors of public companies.[2] Respondents recognize that these risks are interconnected, since a speedy response to a breach can be critical to reputation. "[S]ocial media enable these reputation issues to take on a life of their own, both in terms of viral dispersion as well as uncontrollable timeline, with a footprint that is almost impossible to erase." Yet, close to a quarter of respondents had no plans to address data breaches when they occur, and others stated they were just informally "doing their best."

"Doing their best" may not be enough in today's atmosphere of increasing by serious data breaches. The Identity Theft Resource Center identified 431 total breaches exposing over 11 million records in the first seven months of 2014.[3] Most of the breaches involved businesses – primarily retailers like Target Corp., which was the subject of a number of derivative actions earlier this year on account of its board's handling of a major data breach late in 2013. The EisnerAmper survey noted that overwhelmingly "C-Suite executives and the Board were referenced as the go-to resources to execute a plan to preserve a company's reputation during a crisis," yet directors readily admitted "their lack of understanding of new media and cyber issues – two areas in which mere general knowledge can miss the critical nuances necessary for effective strategic and operational decisions." One respondent noted that most "directors cannot spell IT."

These issues have caused significant concern to shareholders, as evidenced not only by newly filed derivative litigation,[4] but also by the position taken by Institutional

---

[1] http://blogs.absolute.com/blog/cost-data-breach-continues-rise/

[2] *Fifth Annual Board of Directors Survey 2014 – Concerns About Risks Confronting Boards*, http://www.eisneramper.com/IT-Risk-Management-0714.aspx

[3] Identity Theft Resource Center, 2014 Data Breach Category Summary (7/29/2014)

[4] See *Palkon v. Holmes*, No. 14-cv-01234 (D.N.J.) (filed by a Wyndham Worldwide Corporation shareholder charging directors with breach of fiduciary duty after three data breaches resulting in theft of over 600,000 customers' personal and financial data); *Transeo S.A.R.L. v. Bessemer Ventrue Partners IV*, No. 11-cv-5331 (S.D.N.Y.), http://docs.justia.com/cases/federal/district-courts/new-york/nysdce/7:2011cv05331/382774/31/0.pdf?1364657320 (shareholder claim arising from relocation of software

Shareholder Services (ISS) in recommending the removal of Target's chair and other directors who, ISS alleged, failed "to provide sufficient risk oversight" relating to the cyber-theft of customer credit card information.

Recently, SEC Commissioner Luis A. Aguilar spoke on the topic of *Boards of Directors, Corporate Governance and Cyber-risks: Sharpening the Focus* at a New York Stock Exchange conference titled "Cyber Risks and the Boardroom."[5] In line with the EisnerAmper results, Commissioner Aguilar noted that "cybersecurity has become a top concern of American companies, financial institutions, law enforcement, and many regulators." Commissioner Aguilar focused his remarks on "what boards of directors can, and should, do to ensure that their organizations are appropriately considering and addressing cyber-risks." He emphasized that the board's role was primarily one of oversight: "[B]oards are responsible for overseeing that the corporation has established appropriate risk management programs and for overseeing how management implements those programs." These comments harkened back to the SEC's 2009 proxy risk disclosure requirements, which stated that "risk oversight is a key competence of the board."[6] Commissioner Aguilar noted that 2013 proxy filings by companies comprising the S&P 200 revealed that the full boards of these companies are "nearly universally" taking responsibility for risk oversight.

Commissioner Aguilar advised boards to consider a number of changes to deal with cyber-risk management, including:

- Proactively focusing on structural changes, including mandatory cyber-risk education for directors, adequate representation by board members with a good understanding of information technology risks, and a separate enterprise risk committee of the board;

- Identifying appropriate personnel to manage cyber-risk and provide appropriate reports to the board; and

- Establishing a cyber-risk management program, including identifying personnel who are primarily responsible to respond to a cyber-attack and developing a well constructed and deliberate response plan, as well as

---

company's web services from France to the U.S., allegedly disrupting services, compromising client security, and facilitating hacking; violation of European data-privacy laws held to adequately plead a claim for breach of duty of loyalty under Delaware law).

[5] http://www.sec.gov/News/Speech/Detail/Speeck/1370542057946

[6] Proxy Disclosure Enhancements, SEC Rel. No. 33-9089(Dec. 16, 2009), 74 Fed. Reg. 68334. See also *CF Disclosure Guidance: Topic No. 2, Cybersecurity* (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm, specifically discussing the SEC Division of Corporate Finance's view regarding disclosure obligations for cyber-risks and breaches.

> identifying "whether, and how, the cyber-attack will need to be disclosed internally and externally (both to customers and investors)."

Meanwhile, the DHS has held a number of working meetings to discuss cybersecurity,[7] including a July 2014 Insurance Industry Working Session, which resulted in a number of useful suggestions for creating appropriate insurance vehicles to protect companies and directors from the fallout of the data breaches. Many insurance policies currently except liability for losses resulting from a violation of a "right of privacy," and so might not cover data breaches. As a result, the industry is attempting to structure new products that would more adequately meet current needs in this area. The participants at the conference discussed addressing cybersecurity in the context of broader ERM initiatives, appearing to view more generalized ERM insurance policies as the best vehicle to address the costs associated with data breaches. Nevertheless, they recognized barriers to successful ERM programs, particularly for mid-size and smaller companies, including lack of resources, fear of having to address cyber vulnerabilities that might be revealed, communications breakdowns between IT and non-IT security professionals who "use very different language to express basic risk concepts," and difficulties associated with extending in-house ERM programs to vendors. One insurance industry participant suggested that the SEC could positively influence this process by integrating more mature ERM-related best practices into existing regulatory regimes for public companies.

As have previous commentators, both Commissioner Aguilar and the DHS insurance industry panel noted the impossibility of applying a "one-size-fits-all" approach to managing cybersecurity. For directors, this means that only a role-up-your-sleeves, individualized approach tailored to each particular entity can be successful to manage potential fiduciary liability exposure in the long term.

[7] Reported at http://www.dhs.gov/publications/cybersecurity-insurance.