BerkeleyLaw
UNIVERSITY OF CALIFORNIA
Berkeley Center for Law, Business and the Economy

University of California, Berkeley
School of Law
2850 Telegraph Ave, Suite 500
Berkeley, CA 94705-7220

Ph: 510.642.0532 – Fax: 510.643.7095
E-mail: BCLBE@law.berkeley.edu
http://www.law.berkeley.edu/bclbe.htm

Cybersecurity in the Boardroom: New Horizons

By Amit Elazari, LL.M. | April 18, 2017

Cybersecurity risks are growing. As society produces more lines of code, and everything – from cars to sex toys is becoming connected: more vulnerabilities are produced daily, inviting more data breaches. The costs associated with security breaches, mostly reputational, have increased in terms of legal and pure losses of revenues as well. The new oil, is not just data – its security vulnerabilities traded on legitimate and outlawed markets.

The rapidly changing cyber landscape is creating new types of cyber risks, which directors simply cannot continue to ignore. If they do ignore them – they might be slapped with a shareholders' derivative lawsuit in the case of a breach, claiming that management breached its fiduciary duty towards the corporation by failing to monitor the cyber risk.

Cyber is becoming a subject regularly discussed in board rooms, and a critical corporate governance concern. Recent research done by the U.S. National Association of Corporate Directors (NACD) reported that while directors acknowledge the importance and prominence of cyber risks, they also believe that "their boards *do not* possess sufficient knowledge of this growing risk."

In light of these findings, the NACD issued a new report detailing five key principles that directors can adopt to enable oversight over cybersecurity risks: (i) approaching cybersecurity as an "enterprise-wide" managerial risk, (ii) understanding the legal implications of cyber risks, (iii) enabling access to cybersecurity expertise, and discussing cyber risks in the boardroom regularly, (iv) establishing an enterprise-wide cyber-risk management framework and (v) managing cyber risks and terms of deciding which risks to avoid, manage or mitigate through cyber-insurance. Implementing an independent monitoring system, such as Bug Bounty Programs, could also enhance the directors' ability to oversight security risks.

While the NACD report might provide directors with advice on how to oversee cyber risks, other developments in the "cyber-corporate" arena suggest that directors should take a more proactive managerial approach to cyber risks, one that requires them to have genuine expertise in this field.

First, New York adopted a new comprehensive cyber regulation for financial services companies regulated under the New York State Department of Financial Services, effective March 1, 2017 (with a transition period, § 500.22). The newly adopted 23 NYCRR 500 Cybersecurity Requirements require covered entities, among others, (1) to conduct periodical risk assessments, (2) to implement a cybersecurity policy that evaluates the effectiveness of the corporations' cybersecurity program and (3) to conduct periodic penetrations testing and vulnerability assessments. Most importantly, the 23 NYCRR 500 regulations mandate directors to pay attention to cyber laws, requiring the Chairman of the Board or a "Senior Officer" to personally sign the annual certification confirming compliance with the regulations, the Board or a "Senior

University of California, Berkeley
School of Law
2850 Telegraph Ave, Suite 500
Berkeley, CA 94705-7220

Ph: 510.642.0532 – Fax: 510.643.7095
E-mail: BCLBE@law.berkeley.edu
http://www.law.berkeley.edu/bclbe.htm

Officer" to approve the cybersecurity policy, and the Board to receive annual reports from the chief information security officer.

Second, a new bill proposal, the Cybersecurity Disclosure Act of 2017, seeks to mandate public companies to disclose to investors information relating to its directors' expertise and experience in the field of cybersecurity as part of their annual reports/proxy statements. If the company's Board has no such expertise, it is required to disclose "what other cybersecurity steps" it's senior management has taken. It's plausible that companies will prefer to comply with the first requirement, rather than disclosing their detailed cybersecurity strategy and subjecting it to scrutiny and prying eyes.

All of this suggests that directors will be mandated to take a more proactive role on cyber, one which doesn't sum up to "oversighting", or else they might find themselves personally liable.