Bloomberg BNA

Corporate Governance Report™

BNA Insights

Cyber Risk and the Board of Directors—Closing the Gap

BY MICHAEL A. GOLD

The responsibility of corporate directors to address cyber security is commanding more attention and is obviously a significant issue. Yet here is how one writer entitled her Forbes article about the 2012 Carnegie Mellon Cylab Report: ''Boards Are Still Clueless About Cybersecurity.''

Corporate boards have a duty to protect corporate assets, whatever the form these assets take. Increasingly, corporate assets consist of information. In some companies, digital information constitutes most of the assets of the enterprise. Even in industries not commonly thought of as ''hi-tech''—such as energy and utility companies—computers and software play a major role in finance, management and operations, and the most sensitive and mission-critical functions are, with few exceptions, computerized.

The Cyber Risk Governance Gap

Despite the pervasive significance of cyber security to virtually all companies, a gap exists between the legal exposure presented by cyber risks and the ability of corporate boards to address these risks effectively.

Some statistics illustrate this cyber risk ''governance gap.'' Despite the prevalence of digital information and the vulnerability of companies to cyber security threats, the 2012 Carnegie Mellon CyLab Study reported that, among energy and utility companies:

- 71 percent of boards rarely or never review privacy and security budgets,
- 51 percent of boards rarely or never review security program assessments, and
- 64 percent of boards rarely review top level policies.

Similarly, industrial companies, despite their reliance on digital and computerized assets, made only a modestly better showing in the study than the energy and utility companies. These are troubling statistics in view of the U.S. Department of Homeland Security's report of 198 attacks on critical U.S. infrastructure in 2012. One would hope that the boards of companies that are key players in critical U.S. infrastructure would play a far more active role in overseeing their companies' cyber security efforts.

Corporate boards can be timid about engaging cyber risk because the nature of these risks has no real parallel in the experience of most corporate directors.

This governance gap is vividly illustrated by a comment from a director of a major energy company, who was quoted as saying, ''We'll never be entirely comfortable that we're not going to see a plant blown up—but based on what the experts have told us, we have a 99% comfort level.'' This view reflects a fundamental flaw in the way many people, not just corporate directors, view cyber security—that is, cyber security is a continuum, where if your cyber security measures are at 9 on a 10 point scale, your company is safe. Cyber security, however, is essentially binary—you are, at best, secure only at a moment in time. Because of this essentially binary nature, cyber security efforts cannot be static but must be dynamic in order to be effective.

Why is there a cyber risk governance gap? We explore the reasons by addressing three issues:

Michael A. Gold is a partner of Jeffer Mangels Butler & Mitchell LLP in Los Angeles. His practice involves both corporate counseling and transactions and litigation matters. His clients range from early stage companies backed by private equity funds to major national companies. Michael is co-chair of the Firm's Privacy, Information Management and Data Protection Group. He is also a co-author of Bloomberg BNA's Corporate Practice Series Portfolio 86, **Records Retention for Enterprise Knowledge Management**, *which is available for purchase at http://www.bna.com/records-retention-p6983/.*

 ISSN 1520-7625

1. why governance at the board level is behind the digital threat curve,

2. why boards have current legal exposure to cyber risks, and

3. who will bring these legal exposures home to corporate boards.

Reasons for the Gap Between Corporate Governance and Cyber Risk

The IT 'Confidence Gap.' A recent panel discussion of the National Association of Corporate Directors noted several factors that contribute to the inability or reluctance of many boards to effectively address cyber risk and data security.

- Intimidation—Most directors, especially directors in mature companies, are older and are not as comfortable with digital technologies, especially given the dynamic rate of change in the area.
- Highly technical jargon—In addition to the complexity of the technology itself, the information industry uses jargon and code words that raise barriers to those who are not technically savvy.
- The rapidity of change in the digital environment—The information and digital technologies have very short life cycles, demanding almost constant attention. Corporate directors, however, have their own businesses to attend to and can rarely devote the time necessary to maintain currency in the area.

The net result is that corporate boards can be timid about engaging cyber risk because the nature of these risks has no real parallel in the experience of most corporate directors. Hence, the first gap that needs to be overcome is the ''Confidence Gap.''

Cyber Security Fatigue. Closely related to the Confidence Gap is the impact of the sheer volume of information about cyber risk and information security. There is too much information to assimilate, not enough resources or time to do it and, of course, the availability of the well-known default excuse of ''we have a good IT staff,'' which arguably allows directors to assign responsibility to experts. But good IT is not good cyber security, and good IT often serves goals which arguably are counter to cyber security. Relying on IT for strategic data security can lead to a complacency that may be encouraged by the IT staff itself, who often do not understand all of the risks associated with their own systems or in fact see cyber security experts as a challenge to their authority.

Asymmetric Information and Related Risk. As identified in the 2012 Summary of Proceedings of the Advisory Council on Risk Oversight of the National Association of Corporate Directors, this ''information gap'' may be the most significant of the factors contributing to the governance gap. The board is ''simply unaware of the operational risks occurring at their company'' because they do not know enough to ask the necessary questions of the right people to obtain the information they need. The Confidence Gap, Cyber Security Fatigue and the simple fact that directors are not experts in cyber security makes it difficult for directors to know what questions to ask. This lack of knowledge leads, in turn, to an inability or unwillingness to question or challenge those perceived to have more expertise.

When the insurance industry focuses on a particular kind of risk, that risk must be seen as real, and directors need to pay attention.

Boards' Legal Exposure to Cyber Risk

The responsibilities that corporate boards have for cyber security are not newly-minted. Rather, these responsibilities stem from the duties that corporate directors have owed to their companies and shareholders for many years—the duties of care and good faith, connected, of course, to the safe harbor of the ''business judgment rule.'' How far do these duties extend in the world of cyber risk, where external and internal risks may have existential implications for companies?

A couple of excerpts from a 1996 Delaware Chancery Court opinion in a non-cyber risk case are instructive. The litigation addressed the directors' duty of care to oversee corporate activities and implement adequate internal control systems in a major corporation. The governance principles illustrated in these excerpts easily could play a role in a court's consideration of a claim against a corporate board today for ignoring corporate cyber risks—they could be translated into a claim for failure to maintain data security with little editing:

> But it is important that the board exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility. . . .

and

> Failure to monitor: since it does appear that the Board was to some extent unaware of the activities that led to liability, I turn to a consideration of the other potential avenue to director liability that the pleadings take: director inattention or ''negligence.'' Generally where a claim of directorial liability for corporate loss is predicated upon ignorance of liability creating activities within the corporation, as in *Graham* or in this case, in my opinion only a sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable information and reporting system exists—will establish the lack of good faith that is a necessary condition to liability. Such a test of liability—lack of good faith as evidenced by sustained or systematic failure of a director to exercise reasonable oversight—is quite high. But, a demanding test of liability in the oversight context is probably beneficial to corporate shareholders as a class, as it is in the board decision context, since it makes board service by qualified persons more likely, while continuing to act as a stimulus to *good faith performance of duty* by such directors.[1]

The obligation to maintain an effective information reporting system is directly related to maintaining a secure information system, and the failure to do so is, arguably, a measure of a director's negligence.

Who Will Bring the Legal Exposure Home to the Board?

A title from a recently published article states the obvious: ''Regulators and Plaintiff's Lawyers are Ready to Pounce on Privacy and Data Security Missteps.'' The operative words here are ''plaintiff's lawyers.'' As noted in a 2012 report by Lockton Companies, a major insurance broker: ''The bottom line is that we expect to see an increasing trend in D&O claims filed as a result of data

[1] *In re Caremark Int'l Inc. Derviative Litig.*, 698 A.2d 959, 970–71 (Del. Ch. 1996) (emphasis in original).

  CGR ISSN 1520-7625

breach events, failure of the board and senior management team to prevent breaches, and lack of adequate disclosure surrounding such events.''

When the insurance industry focuses on a particular kind of risk, that risk must be seen as real, and directors need to pay attention.

The Future

Companies would do well to examine the role that their boards play in overseeing the management of cyber risk and determine how board composition and functions can be calibrated to more effectively address the risk. Some obvious steps include:

- Mandatory cyber risk education for directors.
- Focus on developing cyber security competence at the board level, including consideration of candidates with appropriate expertise.
- Creation of a board-level reporting system that gives directors timely and usable information to permit a reliable high-level evaluation of the company's cyber risk profile, defensive strategies and infrastructure.

A frequent critique of Corporate America from the financial meltdown of 2008–09 was that corporate profits were privatized but the risks and losses were socialized. Cyber risk is unlikely to yield the same outcome. Rather, the survivors in the world of corporate cyber risk will be those who close the cyber risk governance gap well before it's time for a government bailout.