Cyber Risks For The Boardroom

Heidi Lawson and Daniel Harary - Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.

The Recent Increase In Focus on Privacy Issues

Privacy issues have been the focus of many state efforts over the past few years. However, the SEC has increased their focus tremendously over the past few months (see our blog posts here, here, and here). As early as October 2011, the SEC had demonstrated an interest in cybersecurity events by releasing guidance concerning public company cybersecurity disclosures. Otherwise, the SEC had remained relatively quiet. Recently, however, SEC involvement in this area has ratcheted up noticeably. On January 9, 2014, the SEC announced that it "will continue to examine governance and supervision of information technology systems, operational capability, market access, information security and preparedness to respond to sudden malfunctions and system outages." Further, at a March 26, 2014, SEC-sponsored Cybersecurity Roundtable, SEC Chair Mary Jo White stressed "the compelling need for stronger partnerships between the government and private sector" to address security threats. Commissioner Luis Aguilar also emphasized the need for the SEC to gather additional information and "consider what additional steps the Commission should take to address cyber-threats." Further demonstrating its commitment to the fact-gathering mission, and its increasing focus on cybersecurity, the SEC released an April 15, 2014, Cybersecurity Risk Alert containing a list of detailed questions to be posed to more than 50 different broker-dealers. The stated purpose of the questionnaire is to "assess cybersecurity preparedness in the securities industry."

Directors often ask "what questions should I be asking and what areas should I be looking into?" A great starting point is looking at the areas the SEC has decided to focus on. What is your organization's cybersecurity governance? How does your company identify and assess risks? Is it considered the best in class in your industry? How does your company protect its networks and information? What systems and protocols does the company maintain to detect unauthorized activity? Directors would do well to carefully consider these questions, as the SEC's recent actions and focus indicate its commitment to increasing cybersecurity in the securities industry, and with that intent, an increase in enforcement actions is to be expected.

Why Directors Should Be Concerned

A data breach is not a unitary or self-contained event. The fallout from a breach could impact the directors as well. A security breach may lead to an investigation or an enforcement action by the Securities and Exchange Commission (SEC). The SEC may direct its investigation at the directors and subpoena the directors' documents and records. Compliance with subpoenas may be extremely expensive and, depending upon how the D&O policy defines "claim", there may not be coverage. Moreover, even if the SEC declines to investigate a data breach, the directors nevertheless face exposure to shareholder litigation and, in some cases, investigation by state authorities. Shareholder litigation in the cybersecurity context will typically allege a failure by the board to oversee and prevent the loss. This failure potentially gives rise to oversight liability under Delaware law, where many public companies are incorporated. At least two separate shareholder derivative lawsuits have been filed against Target's directors and officers, alleging breach of fiduciary duty, waste of corporate assets, gross mismanagement and abuse of control. A similar lawsuit was filed in 2010 against the officers and directors of TJX Companies' by its shareholders following a credit card data breach.

Derivative shareholder lawsuits present a large exposure to directors. Given this potential, the trend has been for directors to settle these cases, which has resulted in little guidance from the courts on director liability in the cybersecurity context. Further, there are statutory limitations on the extent to which companies may indemnify their directors for costs, awards or settlements in the derivative litigation context are generally non-indemnifiable by the company in the absence of insurance coverage. Therefore, directors can potentially face large exposures commensurate to the size of the security breach, payment for which will not be reimbursed by the company. Even if the company maintains a D&O insurance policy with adequate limits, many D&O policies contain a standard privacy exclusion (Section IV.D.), which may reduce or eliminate coverage for a cyber breach.

Top Questions Directors Should Be Asking About D&O Coverage

Directors never want to be in the unenviable position of having to seek coverage under their D&O policy. Nevertheless the D&O policy is an indispensable corporate expense, particularly in the case of public companies, where exposures can be much higher. Especially today, when companies are experiencing a meteoric rise in cyber attacks and unauthorized attempts to access data, directors must ensure that that they are covered in the event of a cyber attack, or any other exposure.

The need for a D&O policy is clear: directors and officers potentially face personal liability for lawsuits filed against them, even for alleged acts undertaken on behalf of the company. Although the company may be required or permitted to indemnify the directors depending on the circumstances, in some situations, the company may be prohibited from offering indemnification, or may not have sufficient resources to extend permissive indemnification. Thus, the D&O policy is a director's last resort before personal assets may be invaded. As such, directors should take the time to carefully consider the scope of coverage offered by their D&O policy. The breadth of coverage and policy wording differs significantly from policy to policy and from carrier to carrier.

So, with apologies to David Letterman, here is our "top 10 list" of the questions directors should be asking about their D&O coverage:

1. What is typically covered under a D&O Policy?
2. What are the exclusions that directors should be concerned about?
3. What kinds of situations should be reported to the insurer to trigger coverage and when?
4. Who controls the defense of the director in the event of a claim?
5. Are the policy limits appropriate for the company's risk profile?
6. Does the policy exclude data breaches?
7. Does the policy provide coverage for derivative shareholder claims?
8. How broad is the coverage afforded for regulatory investigations?
9. What is the priority of payments under the policy?
10. What are the potential coverage gaps and how can they be bridged?

If a director really wants to know how the policy will respond in a claim, an independent legal review is always advised. Often policy terms appear to be favorable, but the practical application of that language in the context of an investigation or derivative lawsuit often yields a different result.

Coverage For Investigations

One of the biggest gaps in coverage in D&O coverage today is the lack of meaningful coverage for investigations. Although at first glance the policy language may look like it provides sufficient coverage, the reality is that the way most policies are written, it is almost impossible to trigger coverage in an SEC or Department of Justice investigation simply because the policy language does not match up to the reality of how those investigations are conducted. In the case of a subpoena, one of the costliest components of an investigation, coverage is often only extended for "targets" that are specifically identified on the face of the subpoena. As a matter of course, however, the subpoena target is rarely

identified in this manner, rendering coverage illusory, or in everyday parlance, useless. As regulatory oversight has increased generally in the wake of the financial crisis, and the SEC cybersecurity initiative promises even greater scrutiny, broad coverage for regulatory investigations is a necessity. This is especially true for public companies, as the scope, protocols and frequency of cyber investigations by the SEC and other regulatory agencies remains to be seen.

Companies should look to maximize the availability of coverage for investigations, including costs associated with responding to a subpoena if there is a formal investigation underway. It should be noted that, in addition to arguing that a director or officer is not identified as a target, carriers will typically challenge coverage on the grounds that a subpoena is not a "Claim" under the policy, and/or the policy does not respond to an "informal" information request by regulators. These same challenges are to be expected in the event of an investigation arising out of a data breach. At the most basic level, D&O policies provide coverage for "Claims" made against the company and its directors during the policy period. The amount of coverage provided is therefore reflected in how broadly the policy defines the term "Claim." Companies can therefore guard against insurer challenges and maximize coverage for investigations by ensuring that their D&O policies define a "Claim" in broad terms.

Coverage For Privacy Violations

As we previously noted, recent SEC actions on the topic of cybersecurity indicates increased SEC focus and likely heralds the coming of enforcement actions against public companies for cyber breaches. On the front end, companies can mitigate their risk by ensuring their cyber preparedness in the event of an attack, which, increasingly, appear to be all but inevitable. In the event that a company does suffer a data breach, it will quickly look to its insurance policy to help defray the costs. In theory, litigation arising out of a data breach should be covered under a D&O policy. However, given the rise in hacking and cyber breaches, cyber liability policies have grown in popularity. As a result, D&O policies are increasingly drafted with a standard exclusion for privacy violations and data breaches, some of which has recently changed. Thus companies cannot simply assume that their D&O policy will respond to a cyber breach. Also, the board of directors cannot assume a cyber policy will protect them. Cyber policies may provide some protections, but certainly not for derivative suits or shareholder class actions.

A board should therefore evaluate its insurance program to determine whether adequate coverage is available to respond to a data breach. If the board concludes that its current insurance program is inadequate, there are three available options: first, consider a stand-alone cyber liability policy. Many of these policies offer multiple coverages to respond to a cyber risk, including: security and privacy liability insurance, event management insurance, business interruption insurance, cyber extortion and cyber media insurance. Also, consider an endorsement to D&O policy specifically including coverage for cyber liability risks for the board of directors for oversight liability. Finally, the company may also consider other insurance that may provide some coverage including fiduciary or professional services liability. Again, if the company is unsure of how to interpret its coverage, the company should not hazard an educated guess. Instead, the company should retain counsel to evaluate its risk profile, potential exposure, and adequacy of coverage.

Heidi Lawson, Member, HALawson@mintz.com

Heidi Lawson is an internationally recognized lawyer with extensive experience in corporate governance, bribery and corruption compliance matters, internal investigations, indemnification, and directors and officers and fund management insurance in both the corporate and litigation context.

A significant portion of Heidi's practice is devoted to crisis and risk management and Heidi leads the firm's Crisis Response, Risk Management and Executive Protection Practice. Her practice is international in nature, and she advises companies, brokers, venture capital firms, private equity firms, hedge funds,

family offices, investment banks, and other investment advisors and their senior executives on identifying risks and protecting against those risks. Heidi has helped guide clients through contentious and difficult mergers and acquisitions, data breaches, government investigations, international arbitrations, FCPA and UK Bribery Act issues, corporate compliance matters, product recalls, cyber security, class action litigation, and workplace disasters.

Full Bio (www.mintz.com/professionals/detail/name/heidi-a-lawson)

Daniel Harary, Associate, DSHarary@mintz.com

Daniel Harary focuses his practice on business disputes with a concentration on corporate and professional liability. He has experience in litigation and mediation involving insurance, commercial and employment matters for diverse domestic and international clients. In complex coverage matters, Danny evaluates parties' rights, duties and obligations under sophisticated insurance policies in individual and class action cases involving alleged violations of securities laws, wage and employment laws, the False Claims Act, and consumer protection laws. Additionally, Danny is a member of the firm's Crisis Response, Risk Management and Executive Protection Practice and has experience counseling clients with complex risk management concerns.

Full Bio (www.mintz.com/professionals/detail/name/daniel-s-harary)

Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.

Mintz Levin (www.mintz.com) is an Am Law 100 firm with more than 450 lawyers serving clients worldwide. Applying a cross-disciplinary team approach, we bring attorneys from many different yet complementary areas together to address the rapidly changing legal and regulatory requirements of a wide variety of industries, including Life Sciences; Health Care; Financial Services; Energy Technology; Technology, Communications & Media; and many others. Our major practice areas include Antitrust; Bankruptcy, Restructuring & Commercial Law; Corporate & Securities; Employment, Labor & Benefits; Environmental Law; Health Law; Intellectual Property; Litigation; Public Finance; Real Estate; and Tax.

The firm's eight offices are strategically located to meet the evolving needs of our clients. In addition to our seven US office locations in Boston, Los Angeles, New York, San Diego, San Francisco, Stamford, and Washington, Mintz Levin has an office in London and a liaison office in Israel.