Bloomberg BNA

BNA's
Corporate Counsel Weekly™

The 'Unthinkable' May Need Board Attention

BY MARK KESSEL AND STEPHEN GIOVE

As the Target massive data breach illustrates, plaintiffs' lawyers are increasingly filing derivative and securities fraud lawsuits against companies and their directors based on claims that the board should have recognized and acted on certain risks associated with the company's business. The lawsuit alleges that Target's board breached its fiduciary duties to the company by ignoring the warning signs that a data breach could occur and participated in the maintenance of inadequate cyber-security controls by the company. Target is not unique, as similar suits for data security and privacy breaches have been filed against Google and others. The basis for liability revolves around whether the event could not have been reasonably anticipated by the directors—i.e., was it a ''black swan'' event—or if there were warning signs that were ignored or inadequately pursued by the board.

Before the 9/11 terrorist attacks or the financial meltdown resulting from the subprime crisis, a court was not likely to hold a board legally responsible for failing to recognize these events as risks which the company needed to address; today such risks are no longer black swans. An increasing number of events could impact a company operating in the current environment and, as their complexity continues to rise, the dissemination of information in crisis situations has become more widespread and instantaneous, and the level of scrutiny of the board by an ever-expanding group of constituencies has increased. Indeed, proxy advisory firm Institutional Shareholder Services has even gotten involved in this realm by including risk oversight in its recommendation criteria.

While a board cannot be expected to foresee every potential disaster that might befall the company, it can, in fulfilling its oversight function, ensure that management has adequately taken account of those events that are foreseeable. Natural disasters such as floods or earthquakes, the sudden death of a CEO, ''bad acts'' by rogue employees, cyber-attacks, data security breaches and other misfortunes are no longer so uncommon as to be unforeseeable.

As the recent Target cyber penetration showed, a breach of cyber security can wreak havoc on a company's business and profitability and engender multiple lawsuits from customers and governmental bodies. Similarly, should banks with ATMs have foreseen that Microsoft would abandon Windows XP, leaving the machines that were not upgraded facing significant security vulnerabilities? In light of the magnitude of recent crisis events, boards need to spend time with management to ensure that the risks facing the company are identified and assessed and plans to manage and investigate these risks are formulated, including plans to deal with foreseeable crises.

As a general proposition, the board of directors is legally obligated to discharge its duties in good faith and in accordance with the best interests of the corporation, acting with appropriate loyalty and care. While it is not sufficient to focus solely on the company's financial performance, the board is not required to micromanage the company's operations in fulfilling its oversight obligations. The board should assume, however, that while it need not address events that would not have a significant impact on the company or that are too remote to require attention, its oversight does include an obligation to ensure that safeguards have been implemented to address foreseeable events. In the end, boards are facing risk management decisions—i.e., how much focus, time and money to devote to the oversight of specific risks which they have identified as warranting more attention.

As a starting point, the board should have management identify significant risks to the company's business and operations and present the particular safeguards the company has established to mitigate those risks. Management should present existing crisis management plans to the board so directors can assess their scope and adequacy. As a company's size and complexity change, existing plans may be materially deficient. Therefore, the board or its designated committee needs to review these plans periodically and have management update them regularly.

Mark Kessel was the managing partner and is currently of counsel at Shearman & Sterling LLP. Stephen Giove is a partner in the firm and a founding member of its corporate governance advisory group. The views expressed are the authors' and do not necessarily represent the views of the partners of Shearman & Sterling or the firm as a whole.

 ISSN 0886-0475

While a board cannot be expected to foresee every potential disaster that might befall the company, it can, in fulfilling its oversight function, ensure that management has adequately taken account of those events that are foreseeable.

In performing its oversight of risk, it is critically important that the board ensure that the risk management framework management uses evaluates risks in the context of its assessment of the company's strategic business objectives, as opposed to evaluating risks in isolation. Risk assessment should be ''strategy-centric'' as opposed to ''risk-centric''—i.e., the company's strategic business objectives should be evaluated for the risks that they present, rather than identifying risks and then determining the extent to which they could impact the company. A few of the more common areas that boards now review include the following:

■ *IT Infrastructure* — In addition to cybersecurity, does the company adequately address data privacy and IT security, including issues created by the increase in the use of cloud computing, social media and a multitude of mobile platforms, as well as the proliferation of personal devices used by employees in the workplace? In addition, does the board understand their company's disaster recovery plan and the potential impacts it may have on the company's business?

■ *Regulatory Landscape* — The number of regulations companies are subject to, especially those doing business overseas, has risen dramatically in the past several years. In addition, regulators, ever seeking increased revenues through fines and settlements, are more aggressively enforcing regulations, thereby increasing the importance of having an effective compliance program.

■ *IP/Confidential Information* — In today's global economy, a company's intellectual property and confidential information are key ingredients to its value. Does the company have an adequate program to protect its intellectual property?

■ *Corporate Social Responsibility* — How will the company's reputation or brand identity be negatively impacted if the company does not adequately address social issues such as the environment?

■ *Product Recalls* — Product recalls or defects not only have an immediate impact on a company's earnings, but could also subject it to liability to consumers and governmental bodies, as illustrated by the recent $1.2 billion fine the Justice Department levied against Toyota for withholding information related to its products' safety. The proper handling of a recall, as the J&J Tylenol cyanide tampering example indicates, can avert a major reputational disaster. The recent General Motors handling of its fatal accident cases is another example of the need to have an effective crisis management plan in place. Fatalities associated with a company's products or disasters present many challenges. However, some fundamental procedures should be in place to avoid publicity blunders. For example, it does not take a PR guru to tell a company not to inform families of loved one's death by text messaging, as Malaysia Airlines is reported to have done following the recent loss of one of its planes.

■ *Executive Compensation* — Does the structure of the company's executive compensation program appropriately balance the incentives given to senior management with the risks embedded in the company's corporate strategy?

■ *Shareholder Activism* — In the past several years, an increasing number of hedge funds and other institutional investors have engaged in shareholder activism with an expanding group of companies. Given the sophistication and breadth of activist's toolboxes, no company is immune to an approach by an activist investor. Each company should analyze its business, financial affairs and governance practices to assess which areas are at risk for attack and should develop action plans that could be used if such an attack materializes to avoid adversely impacting the company's business and shareholder value.

■ *Employee Matters* — Does the company have adequate policies and procedures in place regarding the use of social media by employees and restrictions on the communication of confidential information to third parties? If the company has employees who are unionized, what is the nature of the relationship with the union and when is their contract up for renegotiation?

■ *Political Contributions* — As the constraints on political contributions by corporations have decreased, companies are becoming more engaged in the political arena. However, such involvement is not without its risks if management takes a stand on, or directs funds to, controversial issues that can impact its reputation. As a recent example, the CEO of Mozilla resigned after employees complained about his $1,000 contribution to support a 2008 California ballot initiative to ban gay marriage. Boards also need to be vigilant that the company's attempts to influence legislation or regulations, or support candidates, are appropriate to avoid tarnishing the company's reputation.

■ *Insider Trading* — Dealing with analysts and investors in the current environment is also not without risks, as regulators are increasingly focused on trading on inside information. The board should inquire if the company has the requisite policies in place to minimize the likelihood an insider trading problem would occur as well as to assist the company in defending against an enforcement action by the Securities and Exchange Commission, potential lawsuits and an attack on its reputation.

■ *Insurance* — Are the scope, exclusions and amounts of insurance coverage adequate for the company's operations? Does the insurance cover business interruption? Is the Directors and Officers insurance policy adequate in light of the legal exposure?

■ *Reputational Risks* — Does the company understand any reputational risks associated with working with the company's business partners, including with respect to its supply chain?

■ *Disclosure of Significant Risks* — Does the company disclose material risks in public filings to avoid potential lawsuits?

Some practical steps that boards can take to deal with the ever-increasing need for risk oversight include:

■ *Tone at the top* — The board should make management aware of the seriousness with which the board views its risk oversight function. It needs to make clear to management that it expects accurate assessments of the risks in the business, that they are being adequately addressed, and

CCW ISSN 0886-0475

that any material issues that arise are brought promptly to the board's attention.

■ *Benchmarking and best practices* — There are a number of publications that focus on risk oversight by boards, such as the report issued by the National Association of Corporate Directors's Blue Ribbon Commission on Risk Governance and the Governance Center of the Conference Board entitled ''Risk Oversight: Evolving Expectations for Boards.'' These and other sources can assist boards in benchmarking against peers and discerning best practices. In addition, outside consultants can be engaged, if necessary, to assist the board in identifying risks and establishing appropriate oversight functions.

■ *Allocation of oversight responsibilities* — Some financial institutions are by regulation required to have risk management committees. Other companies need to clearly delineate which committee of the board is responsible for which risk identified by the board as warranting board attention. While the audit committee will be responsible for many of the risks discussed above, other committees may have better insights into the risks and should be clearly allocated the responsibility.

■ *Annual review by board or committees* — There should be a report from management on risk and whether developments in the company's business or the environment in which it operates have changed the risks associated with its business to an extent that it requires a change in the board's oversight role.

As the above examples indicate, it does not take a disaster of major proportions to have an adverse impact on a company's business, financial performance or reputation. In the exercise of their oversight obligations and to avoid potential liability, directors should at least assure themselves that the company's management is prepared for events that are reasonably foreseeable. The fact that an event had a major negative impact on a company is not in and of itself a basis to hold directors liable. A court may absolve directors for failing to anticipate a risk where there weren't enough red flags associated with such a risk.

But if, for example, a foreign governmental authority starts to target companies in an industry for bribery by its employees, should boards of companies in other industries perceive such action as a red flag and have management address this type of risk? The Chinese authorities investigated a number of pharmaceutical companies for bribery charges relating to their sales operations in China. What if the Food and Drug Administration starts to step up treating violations of manufacturing problems as criminal offenses; should the board take this as a foreseeable event and start to get involved? These situations present an important reminder that the board needs to be vigilant so it will not be caught as having ignored red flags and be at risk for not having taken appropriate measures to address them.