CORPORATE GOVERNANCE

Cybersecurity Must Be High on the Board Agenda

David A. Katz and Laura A. McIntosh, New York Law Journal

May 24, 2017

David A. Katz and Laura A. McIntosh

Recent global cyberattacks have rudely reminded corporate America that cybersecurity risk management must be at the top of the board of directors' corporate governance agenda. Companies have no choice but to prepare proactively, while directors must understand the nature of cybersecurity risk and prioritize its oversight. Preparation, monitoring, emergency response, and disclosure are topics that boards should consider regularly to properly oversee cyber-risk management. Boards should receive periodic updates from management and its expert advisors on the rapidly developing regulatory cybersecurity environment and on the company's compliance with applicable cybersecurity standards.

Regulatory Environment

A wide range of regulatory efforts are underway with respect to cybersecurity. President Trump signed an executive order this month requiring federal agencies to proactively assess and manage their cybersecurity risks; while the order does not apply to public companies, it highlights the importance of vigilant attention to addressing cyber threats.

Federal banking regulators are in the process of establishing cyber-risk management standards for major financial institutions. And on Capitol Hill, a draft bill was introduced last year that would apply Sarbanes-Oxley certifications and internal controls requirements to a company's information and technology systems and cybersecurity-related controls; while its passage is unlikely, it indicates legislative attention to this issue.
The Securities and Exchange Commission is expanding its focus on cybersecurity. The Enforcement Division has pursued charges in several cases relating to failures to adequately protect customer data, and the SEC's Office of Compliance Inspections and Examinations indicated that reviewing cybersecurity compliance procedures and controls would be a priority in 2017. The SEC has expressed support for the widely utilized NIST Framework, indicating that boards should work with management to ensure that their corporate policies conform to the Framework's guidelines, which are in the process of being updated.

At the state level, the New York State Department of Financial Services recently implemented detailed regulations requiring entities authorized under New York banking, insurance, and financial services laws to establish and maintain a cybersecurity program that meets certain standards, including risk assessment, compliance documentation, and reporting of cyber-events. The cybersecurity program must be based on the covered entity's risk assessment and designed to perform core cybersecurity functions. Other states may follow suit.

Corporate Preparation

The board should be briefed regularly on the company's preparations with respect to cybersecurity and should evaluate the company's preparatory measures against applicable regulatory requirements and the NIST Framework. Although it is widely recognized that even first-rate preparation will not prevent all attacks in this rapidly evolving field, nonetheless it may enable a company to minimize harm, mitigate losses, communicate effectively with stakeholders, and recover as quickly as possible from a cyberattack.

State of the art technological defenses, monitored continuously and updated frequently, possibly with ongoing assistance from outside technological consultants, are essential. Employees at all levels should be trained to follow cybersecurity best practices and protocols in order to recognize threats in the early stages. Prompt recognition and action can forestall large-scale attacks and prevent malicious software from propagating. Having an established relationship with the FBI and other relevant law enforcement resources facilitates immediate reporting and management of an attack.

Preparation should include a detailed emergency response plan. Ideally, this plan should be updated frequently and periodically tested with cyberattack simulations to ensure that both technology and personnel are adequate to the task. Key employees should understand their precise roles, and management should clearly establish the company's priorities in responding to an attack. A shared understanding of goals and values will help to guide employees and outside consultants as they make real-time decisions in the midst of developing situations. Pre-incident retention of response resources such as technology

experts, lawyers, and public relations consultants are important steps to streamline crisis response.

Disclosure of cyberattacks has been minimal in recent years—very few corporate targets publicize the incidents—but it is likely to expand as attacks increase in number and severity and regulatory regimes impose greater disclosure obligations. If a data breach or other cyber-event is arguably material in its effect, nondisclosure can create regulatory enforcement and litigation risk. In the event of an attack, boards should seek the advice of internal and outside counsel in determining the timing, nature, and form of company disclosure.

There is a growing sense that prompt and detailed disclosure is essential to our nation's defense against cyberattacks, particularly in the financial institutions context. Last year, the Department of the Treasury's FinCEN issued an advisory on the reporting of cyber-events and cyber-enabled crime under the Bank Secrecy Act. The advisory emphasized that the voluntary reporting of events (beyond mandated reporting requirements) is highly valuable to law enforcement efforts. Moreover, disclosure and information sharing are likely to be helpful to other institutions facing similar threats or attacks.

Managing the Threat

Increasingly sophisticated cyberattacks are, unfortunately, a fact of life in today's business environment—the question is not "if" a company is going to be attacked, it is really just a question of "when" the attack will come. The challenge for directors is to oversee management's efforts to address cyber-risk and to do their best to ensure that the company is prepared to weather a cyberattack. Cybersecurity consulting firms can be helpful in developing, updating, and stress-testing corporate response plans. In certain industries, a board may wish to have a director who is knowledgeable about cybersecurity, or to create a separate technology committee whose responsibilities include cyber-risk oversight.

Directors should be aware that cyberattacks are increasingly malicious and dangerous as national security issues become ever more entwined with the functioning of American commerce. Unfortunately, cyber-tools developed by state actors (such as the National Security Agency) have been compromised and are being used for commercial gain. Boards should ensure that company insurance policies are adequate to cover previously unknown cyber-threats, as well as extortion and even physical harm to employees.

Boards must review cyberattack preparedness on a regular basis, including business continuity plans, in light of each company's particular vulnerabilities. The best defense—from attacks, from the attendant consequences, and from subsequent litigation—is a carefully tailored and constantly updated protective scheme accompanied by a detailed response plan.

David A. Katz is a partner at Wachtell, Lipton, Rosen & Katz. Laura A. McIntosh is a consulting attorney for the firm. The views expressed are the authors' and do not necessarily represent the views of the partners of Wachtell, Lipton, Rosen & Katz or the firm as a whole.