BAILEY | CAVALIERI

CYBER RISKS: NEW FOCUS FOR DIRECTORS

Cyber risks have become a major potential loss exposure for most corporations. Although nonexistent just a few years ago, most companies today are vulnerable to a growing list of threats relating to technology misuse. Not surprisingly, as businesses have become more reliant on technology, the resulting risks have become far more complex and potentially harmful.

Threats from hackers, thieves, third-party contractors, competitors and employees, as well as inadvertent misuse or loss of data, present potentially catastrophic financial and reputational risks to companies today. Even the most vigilant company can be a victim of a data breach or other cyber loss. Class action lawsuits, huge forensic and mitigation costs, notification and credit monitoring services and data restoration efforts can result in tens or even hundreds of millions of dollars of loss to a company. State attorneys general, federal and state regulators and plaintiff lawyers are all likely and formidable adversaries to the company if something goes wrong. In addition, the company's computer systems may need to be shut down and business operations may be interrupted.

Like any other major risk exposure, directors should monitor the company's cyber risks and confirm that reasonable steps are being taken to identify, prevent, mitigate and respond to cyber-related problems when they arise. Because these risks can damage not only the company but its customers, suppliers, other constituents and even the public, extra caution is necessary. Plus, new federal and state statutes and regulations are being adopted with increasing frequency which mandate appropriate company risk management practices in this area.

Directors are not expected to fully understand all of the risks, and all of the company's risk management responses, in this highly technical area. However, directors should at a minimum comply with laws expressly applicable to them, should ask informed questions to gauge the company's focus and preparedness in this area, and should generally understand the extent to which the company is insured—or not insured—for these exposures. The following discussion summarizes (i) voluntary Guidelines issued in February, 2014 by the National Standards and Technology to reduce cyber risks to critical infrastructure, (ii) guidance from the SEC relating to cybersecurity risk disclosures, (iii) a sweeping FTC rule relating to identity theft protection programs which requires board of director action, and (iv) various questions a reasonably diligent director could ask to assure the company's cyber risks are being properly addressed.

1. Critical Infrastructure Cyber Guidelines

In February 2013, President Obama issued Executive Order 13636, which directed the National Institute of Standards and Technology ("NIST") to work with critical infrastructure owners and operators in developing a "Cybersecurity Framework" that captures industry best practices to reduce cyber risks to critical infrastructure. Under the Executive Order, the Secretary of Homeland Security was tasked with establishing a "voluntary program" for implementation of the Cybersecurity Framework in the critical infrastructure industries, and developing incentives to encourage participation in the program by those industries, as well as others.

In February 2014, the NIST issued its finalized Framework for Improving Critical Infrastructure Cybersecurity ("Framework"). The Framework, which is primarily directed to senior management and directors of companies in critical infrastructure industries, was developed with input of public and private sector organizations and is intended to reflect current industry sector standards, guidelines and best practices.

The Framework is voluntary and its stated purpose is not to replace existing sector standards or add an unnecessary layer on existing standards and practices. But, many believe at least some modified version of the Framework will be incorporated into commercial contracts for critical infrastructure. Plus, plaintiff lawyers will likely contend the Framework reflects a minimum standard of care for cybersecurity.

"Critical Infrastructure" is defined in the Framework as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health and safety, or any combination of those matters." Industries specifically referenced as having critical infrastructure include financial services, energy, communications, healthcare, utilities, transportation and food/agriculture.

The Framework is not industry specific and seeks to protect critical infrastructure from cyber risks by describing a certain minimum level of cybersecurity. Risks are organized in the Framework around five core activities that a company's management and IT security teams routinely should perform when dealing with security risks: identify, protect, detect, respond, and recover. For each of these core activities, the Framework summarizes processes and best-practices that create standards for assessing and managing risks posed by cyber threats.

2. SEC Disclosure Guidance

On October 13, 2011, the SEC's Division of Corporation Finance released "CF Disclosure Guidance: Topic No. 2 – Cybersecurity." That "Guidance" summarizes the SEC's views regarding a company's disclosure obligations relating to cybersecurity risks and incidents. It does not change existing disclosure law, but merely explains the SEC's interpretation of that existing law to the evolving topic of cybersecurity.

The Guidance defines "cybersecurity" as "the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access." The Guidance recognizes that no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, but that "a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents." The Guidance also notes that material information regarding cybersecurity risks and cyber incidents "is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading." The Guidance then highlights the following specific disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents:

- Risk Factors. Consistent with the Regulation S-K Item 503(c), cybersecurity risk disclosures must adequately describe the nature of the material risks and specify how each risk affects the registrant. The Guidance specifically mentions that to the extent material, appropriate disclosures may include a description of relevant insurance coverage.

- MD&A. Registrants should address cybersecurity risks and cyber incidents in their MD&A if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect.

- Description of Business. If one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions, the registrant should provide disclosure in this section.

- Legal Proceedings. If a material pending legal proceeding involves a cyber incident, the registrant may need to disclose information regarding such litigation in this section.

- Financial Statements. The Guidance reviews a number of situations in which cybersecurity risks and cyber incidents could impact a company's financial statement disclosures, including disclosures regarding accounting treatment, depending on the nature and severity of the actual or potential incident.

- Disclosure Controls and Procedures. Registrants are required to disclose conclusions on the effectiveness of disclosure controls and procedures.

The Guidance is not a new disclosure rule and should not be viewed as creating additional disclosure obligations, or expanding a public company's existing disclosure obligations, regarding cybersecurity. However, in any shareholder litigation arising from a cyber incident, plaintiffs will undoubtedly challenge the disclosures based on this new Guidance.

The intent and focus of these new Guidelines is to provide better clarity to public companies with respect to what disclosures are required by existing laws and regulations with respect to cyber risks and incidents. Obviously, the SEC wants shareholders to be informed about what harm has or could occur to the company with respect to cyber matters. In making those disclosures, the SEC recognizes that a company may need to disclosure what relevant insurance coverage the company maintains in order to put the risk disclosures into proper context (i.e. the existence and disclosure of insurance will tend to offset some of the potential harm to the company arising from the cyber risks being disclosed).

This new SEC Guidance, by itself, should not materially impact a company's insurance purchasing decision. Like other areas of risk management, the ultimate question is whether a company believes it is prudent to transfer some of its cyber risk via an insurance product. That is a classic business decision that typically is protected from judicial second-guessing via the business judgment rule. The SEC is not now suggesting that companies should or should not purchase cyber insurance, but is merely stating that in order to present a full picture of a company's "net" cyber exposure, a description of any relevant insurance coverage may need to be included in the company's cyber disclosures.

Companies are struggling with how to respond to this new SEC guidance since cyber risks and cyber incidents are so difficult to predict, evaluate, quantify and describe. However, it is clear that there will be more cyber-related disclosures in the future than has occurred in the past. Because of that, companies may want to mitigate shareholder concerns arising from those additional cyber disclosures by purchasing and disclosing the existence of cyber insurance. Although disclosing insurance information in some contexts is not desirable because it may serve as a lightning rod for claims against the Insureds, that risk here should be minimal since most of the loss covered by a cyber policy would very likely be incurred with or without the policy existing and being known by third parties (i.e., the disclosure of a company's cyber insurance should not attract claims that would not otherwise be filed as a result of a covered cyber incident).

3. FTC "Red Flags Rule"

Effective December 31, 2010, the so-called FTC "Red Flags Rule" (16 CFR 681) requires a wide variety of companies to adopt Identity Theft Protection Programs that identify warning signals which should alert a company to the risk of identity theft, and that detect, mitigate and deal with identity thefts when they occur. Importantly, the new Rule states that the Identity Theft Protection Program must be approved by the company's board of directors or an appropriate committee designated by the board.

This new Rule applies to financial institutions and "creditors" with "covered accounts." A "creditor" is broadly defined to mean "any person who regularly extends, renews or continues credit." This definition appears to cover a wide variety of entities (including public utilities) that extend credit or give credit terms, such as permitting payment at the end of the month for goods or services rendered throughout the month. As a result, any company that permits deferred payments appears to be a "creditor" under this new FTC Rule. For example, if

the company issues a bill and receives payment subsequent to the provision of the goods or services, that company probably is a "creditor" under this Rule. A "covered account" is likewise defined very broadly in the Rule to include an account offered primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions. A "covered account" also includes any business account if identity theft with respect to that account presents a reasonably foreseeable risk to consumers or to the safety and soundness of the company.

Under the Rule, larger and higher-risk entities must have a more comprehensive Identity Theft Protection Program than smaller or lower-risk entities. These Programs must include the establishment, testing and deployment of an effective program to identify and act upon "red flags" which alert the company to identity theft or the potential for identity theft. Merely adopting a program without proactive enforcement and oversight does not satisfy the Rule. Directors should carefully review the Identity Theft Protection Program recommended by management and should, before approving that Program, assure themselves that the Program is reasonably robust, sufficiently tailored to the unique circumstances of the company, is properly funded and staffed, and will be periodically reviewed by senior management and the board for effectiveness.

4. Cyber Risk Questions for Directors

For many companies, cyber risks represent one of the most volatile and potentially damaging exposures to the company. However, because these risks are so new, evolving and complex, many boards have given little if any attention to these risks. Although each company faces unique cyber risks and therefore each company's response to these risks should be unique, the following summarizes 10 important questions which directors could ask in order to better understand these risks and whether the company is adequately responding to these risks.

1. Is the responsibility and accountability for the creation, implementation, enforcement and updating of an integrated and company-wide cyber risk management program clearly defined at the executive level?

2. Does the management team which addresses cyber risks include senior representatives from executive management, IT, legal, risk management, public relations and compliance/audit?

3. Is the overall cyber risk management program periodically reviewed by the board?

4. Does a board committee have designated oversight responsibility for the cyber risk management program?

5. What are the company's greatest cyber risks and how are those risks being anticipated, managed and mitigated?

6. Is each component of the cyber risk management program documented, frequently tested and periodically audited by independent experts, and what are the results of that testing and audit?

7. Are protocols for reacting to a cyber risk crisis when it occurs well defined and broadly understood?

8. Are all employees required to participate in regular education and training programs relating to cyber risks?

9. What is the company's budget and staffing for cyber risk management and how does that compare with peer companies?

10. What, if any, insurance coverage does the company maintain for cyber risks and is that coverage adequate in scope and amount?

About the Author:

Dan A. Bailey is the Chair of the Firm's Directors & Officers Liability Practice Group and represents and consults with directors and officers, corporations, insurance companies, and law firms across the country. In addition to advising Boards and drafting most of the D&O insurance policies in the market, he has represented clients or served as an expert witness in many of the largest D&O claims for more than 30 years. He is co-author of Liability of Corporate Officers and Directors, a leading treatise on the topic, has published dozens of articles and speaks at more than 20 seminars a year on the subject.

He can be reached at (614) 229-3213, or dbailey@baileycav.com*.*