SPECIAL FEATURE

CYBERSECURITY THREATS: WHAT EVERY DIRECTOR SHOULD KNOW ABOUT BOARD RESPONSIBILITIES AND OBLIGATIONS

By Thomas W. Jenkins, Benjamin P. Sykes and Molly McGinnis Stine

Thomas W. Jenkins is a Partner in the Insurance and Business Litigation groups of Locke Lord LLP. He represents insurance clients on a broad range issues, including regulatory, licensing, company formation, compliance, and Board responsibilities. He also works in the area of insurance company liquidations and rehabilitations.

Benjamin P. Sykes is a Partner in the Insurance group of Locke Lord LLP where he practices insurance, health care and administrative law. He advises insurers, organizations, health care providers, state agencies, managing general agents and third party administrators on complex issues relating to compliance with various federal and state insurance laws and provides counsel on transactional matters.

Molly McGinnis Stine is a Partner and Co-Chair of the Privacy & Cybersecurity Group of Locke Lord LLP. Her representation of insurers and reinsurers has involved professional liability, directors and officers, errors and omissions, and financial liability claims. In particular, Molly focuses on cyber, privacy, data security, communications, social media, and other evolving risks.

Every director and officer fears the 2AM phone call. In the past, those calls usually dealt with large class action suits, SEC investigations or even possibly natural disasters impacting major operation centers. Now a new fear has been added to the very top of that list: a cybersecurity hack. However, there are steps the boards of guaranty funds can take to ensure that when that 2AM call comes, their organizations are prepared to respond to such a cybersecurity incident.

While board of director responsibilities with respect to an organization's cybersecurity obligations are still evolving, certain standards have been developed through case law, regulation and best practices. And while the majority of these standards are primarily applicable to publicly traded corporations and insurance companies, not guaranty funds, they represent "best practices" that the boards of guaranty funds may be held to by plaintiff attorneys or attorneys general in the event of a data breach.

Although these standards do not require every board member to be a technical expert in cybersecurity, they do require an appropriate level of oversight, approval and ongoing review of both cybersecurity policies and threats.

CASE LAW DEVELOPED STANDARDS

The fundamental standard for board responsibility regarding risk oversight, generally, comes from the famous 1996 Caremark decision, which requires boards to assure that companies have an information and reporting system that is reasonably designed to provide accurate information to senior management and the board itself to reach informed judgments. See In re. Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996).

A board only fails to meet its *Caremark* duties if it utterly fails to (i) implement any reporting system or consciously failed to monitor or (ii) oversee its reporting system operations. See Stone ex rel. *AmSouth Bancorporation v. Ritter*, 911 A.2d 362 (Del. 2006). Obviously these are very high standards for failure, and in fact many of the better known cybersecurity breach cases (Home Depot, Wyndham, Target) have been dismissed on these grounds.

STATUTORY- AND REGULATORY-BASED STANDARDS

Within the insurance industry, New York's Cybersecurity Regulation, adopted in 2017, was the harbinger of things to come with respect to state regulation of cyber preparedness obligations. Requiring detailed information about security programs and policies, encryption standards, penetration testing and vulnerability assessments, incident response plan and training obligations for all employees, New York's Cybersecurity Regulation caused significant scrambling by many companies to bring their regimes into compliance. Most significantly for boards, the regulation requires that the security policies of a company must be approved and annually certified by a senior officer or the board of directors (or an appropriate committee thereof).

Although some industry experts had initially hoped that these requirements would be isolated to New York, the National Association of Insurance Commissioners squashed such aspirations when it ditched its own, less onerous, draft Cybersecurity Model Law that it had been working on for years, in favor of new draft Model Law that closely mirrors New York's cybersecurity framework.

In addition, while less directly applicable to the insurance industry, from a federal perspective, regulations promulgated under the 2001 Gramm-Leach-Bliley Act similarly require the board (or an appropriate committee thereof) of a financial institution: (i) approve the company's written security program and (ii) oversee development, implementation and maintenance of the company's information security program. And with respect to public companies, the SEC issued interpretive guidance earlier this year which requires that a company's CEO and CFO provide certification regarding the design and effectiveness of a company's disclosure control and procedures, including disclosure of cybersecurity matters.

PRACTICAL STEPS BOARDS SHOULD TAKE ON CYBERSECURITY ISSUES

In addition to strictly legal requirements, various third party groups and trade organizations have attempted to develop various standards and best practices for board oversight of cybersecurity risks, the most notable of these being the National Association of Corporate Directors' "Handbook on Cyber-Risk Oversight."

The Handbook identifies five key steps that boards should take to address cyber risks:

- Understand cybersecurity
- Understand legal implications of cyber risk
- Ensure adequate board access to cybersecurity expertise
- Ensure adequate staffing and budget
- Address cyber risk

From a governance perspective, every board should also:

- reserve adequate time on its agenda to discuss cybersecurity issues;
- determine whether the board needs one or more directors with a sophisticated understanding of cybersecurity issues, or whether a specialized committee focused on cybersecurity is necessary; and
- periodically review management's assessment of the company's cybersecurity risks.

Finally, we have provided nine key questions board members should be asking regarding an entity's cybersecurity program to ensure their entities are aligned and prepared to address cybersecurity threats.

9 Questions Every Board Should Be Asking About Cybersecurity

1. Who is in charge of cybersecurity?
2. Have we identified all of our information assets to be protected?
3. Have we identified all 3rd parties that may hold or have access to our information assets and evaluated their security programs?
4. Do we conduct periodic risk assessments?
5. Do we have a written security program?
6. Have we committed sufficient resources and budget to implement the security program?
7. Do we monitor the operation and effectiveness of our security program?
8. Are we prepared to respond in the event of a security breach?
9. Do we have appropriate cyber insurance?

BACK TO THAT 2AM CALL

While there is no such thing as a "good" 2AM phone call, if you and your board have taken the steps outlined in this article, you hopefully can get back to sleep knowing your guaranty fund has an appropriate cybersecurity program and response plan in place to address such breaches and you have appropriately discharged your duties as a director.