CORPORATE COMPLIANCE INSIGHTS

December 19, 2016

# Enhancing Board Oversight of Cyber Risk

## The Board's Increasingly Important Role

By Tod A. Northman and Joseph A. Dickinson

Tod A. Northman is Counsel in the Corporate and Privacy & Data Security groups at Tucker Ellis LLP. He counsels clients of all sizes in a variety of industries, with a particular focus in the areas of aviation, benefit entities and real estate.

Joseph A. Dickinson is Counsel in the Privacy & Data Security group at Tucker Ellis LLP. He is a litigator and counselor with more than 25 years of business and legal experience representing and advising corporations and senior leadership nationally and internationally. Joe has broad experience in the areas of data privacy and security, data breach litigation, HIPAA compliance, intellectual property litigation and technology licensing.

**Following a presidential campaign dominated** by talk of hacked email and unsecured servers, businesses are emphatically reminded of the potential cybersecurity danger no matter the business or industry. Threats come from all directions. Criminals and foreign hackers have grabbed headlines with personal financial data thefts from Target and Home Depot. Yet a 2016 IBM-sponsored study concluded that 60 percent of all attacks come from internal sources, with the majority carried out with malicious intent and a quarter of the breaches resulting from error. Compounding the problem, the damages caused by cyber breaches are skyrocketing: the average cost of a data breach is more than $4 million and growing annually, according to the IBM study.

As the risk grows, the board of directors role in identifying and managing the risk becomes more imperative. The obligation to protect the business is the same as with other business risks, but in this case is overlaid with the obligation to ensure the business's legal compliance. The intersection highlights the opportunity – cybersecurity risk cuts across a business and requires oversight from a similarly multifaceted perspective. The National Association of Corporate Directors' Cyber Risk Oversight Handbook, published in 2014, identifies "enterprise-wide risk management" as an indispensable component of cybersecurity. Boards must echo this viewpoint with a specific focus on the cyber risk management program.

### Get Your Priorities Straight

Establishing ownership for cybersecurity risk is the first step. Ultimately, the board is responsible for ensuring that the organization's cybersecurity program is adequately resourced. A board can delegate governance to a risk committee, but maintaining a businesswide view of the threat is critical. The awareness of the danger must be tempered by a realistic strategy that prioritizes protection of the business's assets. FBI Director James Comey asserted: "There are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese." The threats are too pervasive to be eliminated; instead, businesses must determine which assets to prioritize for protection. This undertaking must start at the board level.

In that light, a risk-based strategy focused only on prevention may divert critical resources from the needed holistic approach to protecting the business's most important assets. A thorough program should address cyber risks at all levels, including infiltration, propagation and exfiltration. The board should require that management ensure regular evaluation and prioritization of assets and the cyber risks to those assets. The board should lead the process of determining the appropriate strategy for identifying and prioritizing the risks, as well as defining the organization's plan for which risks to accept and which risks to mitigate.

### Policies and Procedures

Because internal threats, including human error, constitute such a significant portion of cyber beaches, establishing well-designed policies and procedures for handling electronic information is a critical component of any cybersecurity program. Training employees in how to handle information yields significant benefits. Training helps establish the organization's culture and demonstrates the importance of good cyber practices to the organization. Directors and C-Suite leadership should also receive training and regular updates on the organization's cyber program.

Given the frequency of breaches caused by internal sources, the organization can improve the effectiveness of the cybersecurity program by monitoring

*Continued on back*

and enforcing compliance with policies and procedures. Doing so also helps reinforce the culture of safety. Equally important is making sure that appropriate sanctions are included in the policies to effectively deal with those employees involved with causing breaches.

### Detection and Defense

The bad guys are continually adapting their methods. Consequently, the board should require that the organization periodically evaluate the latest technologies and techniques for responding to cyber attacks and update the board on the results of those efforts. Strategies must be business specific and based on the industry, size of business and type of information processed and stored, among numerous other factors. The board should also be involved with the evaluation of the business's detection systems to ensure that resources are devoted appropriately to respond to the high-priority threats.

### Develop an Incident Response Plan

As a key component of any cybersecurity program, businesses must establish an incident response plan. Being prepared to respond to a cyber breach significantly helps reduce the potential damage by improving the speed and quality of response. Some of the most damaging breaches, such as at Sony, have escalated when the target appears not to understand the threat. This lack of understanding can often be traced to inadequate incident response planning. Having a plan in place enables the business to respond more quickly, mitigating the impact on the data, and also helps the business to identify and initiate the necessary response to regain control. FTC guidance released in the fall of 2016 emphasized that establishing an incident response plan is a critical aspect of any cybersecurity program.

The plan should be detailed, including identifying parties inside and outside the organization who can be called upon to help. The board should facilitate prompt access to adequate cybersecurity expertise in advance. The plan should also document the thresholds that would require reporting a breach to law enforcement or other regulatory bodies. Both the FBI and the Department of Justice have cybercrime units that can be valuable allies in combating or preventing a cyber breach.

Once established, the board should regularly review the plan. The company should consider using tabletop exercises and simulated breaches to test and improve its plan.

The plan ought to require a formal assessment of the damage from any cyber event and that assessment should be shared promptly with the board. The board should use the assessment to evaluate and improve the incident response plan.

The article originally appeared on Corporate Compliance Insights, at:
http://corporatecomplianceinsights.com/enhancing-board-oversight-cyber-risk/