7 QUESTIONS BOARD DIRECTORS SHOULD ASK ABOUT CYBERSECURITY

We are living in an exciting times: digital technologies, mobile devices, cloud computing, big data analytics and social media have brought about immense benefits and opportunities to corporations; however, there is also a "dark side" to these exciting technology developments.

The management of cybersecurity requires Board Directors to consider whether their company is appropriately assessing cyber risks and devoting adequate resources to prevent cyber-attacks. Board Directors are not expected to be experts in cyber security; however, they are responsible for ensuring executive management and employees are thinking in a proactive, predictive and preventative to mitigate cyber threats and risks.

When a cyber-attack strikes corporations incur financial losses, business disruption and negative publicity. More often than not, cyber-attacks are the result of a failure in the corporation's information technology infrastructure, processes, internal controls and/or employees training. Furthermore, cyber-attacks result in substantial response costs, lasting reputational harm and litigation for failing to implement adequate steps to protect the company and its' customers. More recently, we have seen the emergence of derivative cyber security lawsuits brought against attacked companies, their senior executives, and the Board of Directors.

Absolute cybersecurity is an unrealistic goal for a company. As with other categories of enterprise risks, a company must define and set a risk tolerance level for cyber risks. Additionally, Boards should ensure that executive management develops a cybersecurity strategy and well-constructed response plans. As with all response plans, there must regular assessments and discussions of potential attack scenarios. Finally, when a breach or attack occurs there must be a mechanism in place to notify and update the appropriate Board and management committees.

Given the heightened awareness of cybersecurity and technology risks, Directors should ensure that their company is appropriately addressing, monitoring and taking preventative action. Questions requiring clarification include:

1. How do we identify and quantify the impact of cyber related risk exposures on our businesses, products and customers?
2. How many cyber related incidents are detected hourly/daily/weekly and what is the current threshold for notifying executive management?
3. Do we have cyber incident reporting procedures to notify insurers, vendors and customers?
4. What data, and how much, are we willing to lose or have compromised?
5. Are we assessing, analyzing and determining how much cyber risk should be assumed versus transferred using insurance or to third-party vendors?
6. Do we have a comprehensive, real-time crisis response plan in place for cyber threats and incidents? How frequently is the response plan tested?
7. Do we have the right talent in the company as well as clear lines of accountability and responsibility for cybersecurity?

The Board and executive management should also encourage a company culture which views cyber threats as a corporate social responsibility regardless of the equipment, device or media. This can be achieved through employee awareness and training programs that introduce current cybersecurity risks and encourage employees to report probable cyber related threats.

Board oversight of cybersecurity is critical to ensuring corporations are taking adequate steps to prevent, and prepare for, the damage that can result from a cyber-related attack. There can be no excuse by a company for improper preparation, delayed deliberation, or failure to engage cybersecurity risks. Regardless of corporation's size or regulatory requirements, both management and Board committee should ensure the oversight of cybersecurity and cyber risks are a regular agenda item at the risk management or audit committee meetings.