BOARDS NEED TO BE AWARE OF EVOLVING CYBER-LEGAL LANDSCAPE

Boards of directors face several versions of risk from cyber breaches. Obviously, there is the risk of loss or manipulation of the data. There is also a risk of reputational loss. However, regardless of the actual data or reputational impacts boards need to be concerned about legal risks that can occur unrelated to the other risks.

Target's stock price rose by over 30% following its well-publicized data breach and actual financial loss was around .01% of revenue, but they still got sued.

Making this risk even more challenging is the fact that laws and regulations for cybersecurity are in a constant state of flux. Now that cyber breaches seem to be a daily part of the news cycle, it seems as if every governmental agency – state, local, federal, and international – all want to create their own cyber regulatory formation.

New, overlapping, and changing laws are emerging everywhere, including new mandates from organizations that haven't dealt with cybersecurity matters until recently.

Federal agencies that affect sectors such as retail, healthcare, banking and insurance, chemicals, telecommunications, and utilities impose unique sets of requirements for cybersecurity.

States, too – especially when it comes to data breach notification laws – have their own requirements. Because there's little coordination between state legislatures, many post-breach laws hold contradictory requirements on matters such as timeline to disclosure, manner of notification, and baseline company obligations.

At a global level, entities such as the European Union have imposed privacy requirements that can limit cybersecurity activities of multi-nationals. Data localization requirements in China and Russia and other markets can pose other challenges.

Boards of publicly-traded companies likely know the Securities and Exchange Commission since 2011 has urged publicly-traded companies to disclose material information about cyber risks. The commission is under pressure to increase the strictness of its guidance.

What's a director to do? Directors don't need to become legal scholars any more than they need to become technical experts to properly enact their supervisory roles with respect to cybersecurity. However, they do need to be able to document that they are informed of what the legal playing field is for their unique business and they ought to be aware that the field may be shifting under their feet.

For directors, cybersecurity oversight goes straight to execution of fiduciary duty. Without robust oversight, plaintiffs may allege the board neglected its responsibility to confirm the adequacy of company protections against data breaches and other cybersecurity incidents.

Major retailers have paid out to settle class-action lawsuits following consumer data breaches. Federal regulators have taken household-name brands to court for failing to employ data security measures. Surveys show directors and officers anticipate more shareholder lawsuits and a surge in demand by investors for transparency around cyber incidents.

In 2014, and again with a revised edition in 2017, the National Association of Corporate Directors teamed with the Internet Security Alliance to produce a handbook guiding directors in overseeing this difficult terrain. This June 21, NACD, in partnership with ISA, will host a full day event in Chicago that brings together directors, executives, and cybersecurity experts to share real-world insights and critical action steps for boards to foster enterprise-wide cyber resiliency. The second of 5 principles that NACD suggest directors consider as they guide the board's work is to understand the legal implications of cyber risks as they relate to their company's specific circumstances.

Directors are protected in lawsuits by the business judgment rule, but only when the they take reasonable steps to inform themselves. In an age when virtually every organization is vulnerable to a cyber breach, possibly by nation-state affiliated attackers, the mere existence of a cyber breach is not necessarily evidence of inadequate oversight.

Directors don't need deep knowledge about cyber law. But they should be briefed by inside or outside counsel on a regular basis about the requirements that apply to the company. Boardroom minutes should show active discussions about cybersecurity and the legal and regulatory landscape. Regularly scheduled reports from management should enable the board to demonstrate that they have appropriately assessed whether the organizations adequately address potential legal risks.

And companies should consider the appropriate degree of transparency about their cybersecurity processes. The Council of Institutional Investors notes that investors will have greater confidence that a company isn't withholding information during an incident "if it proactively communicates the process by which it assesses damage caused by a cyber incident and the methodology it uses to account for cyber incidents." Making that process transparent shouldn't by itself reveal sensitive information.

The bottom line is that there are a range of cyber threats that boards need to be aware of and a multi-faceted enterprise-wide strategy will be their best protection. Following sound IT standards and practices can go a long way toward protecting the company's data. Thoughtful incident management and communications strategies can assist in protecting a firm's reputation and sensible steps can be helpful in managing the unique legal risks generated by cyber attackers.

Written by Larry Clinton, ISA President & CEO, and David Perera, Assistant Vice-President for Government and Policy