Q&A INTERVIEW WITH EXECUTIVE ALLAN TESSLER

Corporate Directors Must Be Involved in Cyber Security

ALLAN R. TESSLER

Mr. Allan R. Tessler, Esq. is currently Director of online brokerage firm TD Ameritrade, and lead Director and Chair of the finance committee of L Brands, Inc., parent company to the Victoria's Secret, PINK, Bath & Body Works, La Senza and Henri Bendel consumer brands. Allan was also Chairman of the Board of Epoch Investment Partners, Inc.; Board Member and chairman Emeritus of the Hudson Institute; and member of the Board of Governors of the Boys & Girls Clubs of America.

IMPERVA®

CIO
Strategic Marketing Services

FOR MORE INFORMATION GO TO:
imperva.com/go/directors

Why is it important for corporate directors to understand cyber security risks?

A corporate board needs to be responsible for ensuring that an organization's intellectual assets as well as customer information are protected. Customer data is one of the primary sets of information that needs to be safeguarded from hacking and invasion because of the potential mal-use of that information.

What are the costs of poor board oversight of cyber security risks?

The impact of cyber breaches is quite well known. In the retail world Target had problems, while in the healthcare world Anthem was victimized. A number of banks and brokerage firms have had customer accounts looted of money, while others have lost the identities of their customers. All of this is registered very clearly on the minds of public company corporate directors.

How can corporate directors with no technology background learn to understand cyber security risks?

In order to obtain adequate knowledge, directors have to turn either to other people on the board with technological capability or to people inside management – the COO, the CIO, or the CISO. They also need to discuss these issues with company legal counsel, both internal and external.

What's a basic first step directors could take to ensure effective cyber security?

Corporate directors – the board and management – need to prioritize the intellectual informational assets they have. They need to prioritize the level of protection around these assets relative to their importance to the business and the board, as well as to customers or other communities interested in protecting that type of asset. This is a fundamental task of internal analysis that needs to be conducted in every business.

Should every board have a cyber security expert? How about a technology committee?

There are a lot of different approaches. Some businesses get reports from the CIO or CISO. Other companies have a technology committee. In the boards I'm involved with, I have instituted a program where the CIO, the COO, and the CISO either collectively or individually come to every board meeting and address whatever is on their agenda regarding cyber security.

Should corporate directors rely on external audit firms for cyber security awareness?

It's a combination. In two of my boards, we have an outside auditing group come in and review the activities of our cyber security group. They review it on a periodic basis and report back to us. Some businesses I know have retained outside experts either on their risk committee or audit committee to further aid the boards in understanding the performance of their internal activities. Either approach is reasonable.

Are there resources available for corporate directors to better understand cyber security threats?

They can review material on cyber security from director advisory services, law firms or accounting firms. And if the company has engaged an outside cyber security firm, the board can have experts from that firm periodically brief it on how things are going. Getting their viewpoint can be valuable because most of the time boards only hear from corporate insiders.