

U.S. Considers Requiring Companies To Report Their Security Measures

By Harvey Simon

October 15, 2003



The Bush administration is considering requiring public companies to disclose what they have done to protect against terrorist attacks, according to Homeland Security Secretary Tom Ridge.

While the administration has no immediate plans to require such disclosure, officials are looking at the idea "possibly as a requirement down the road," Ridge told Homeland Security & Defense Oct. 9.

Ridge met last week with Securities and Exchange Commission (SEC) Chairman William Donaldson, to discuss the idea of including security measures among the disclosures that publicly traded companies are required to make in their annual reports.

"Staff members at the SEC are working with the Department [of Homeland Security] and examining the issue," commission spokesman John Heine said.

For the information to be meaningful, there needs to be a uniform way to compare the value of security measures among companies within an industry sector, according to Gail Norstrom, managing director of the property practices group at Aon Risk Services Companies, Inc., in Avon, Conn.

Norstrom said he would support a reporting requirement "to the extent that it could be done in a way that the words in one company's report, how they describe things, would have some relative relevance across all reports," with industry groups deciding on the appropriate way of describing their sectors' security measures.

That type of uniform reporting would be harder to accomplish with physical security than cyber security, where such standards already exist, Norstrom said.

But Bob Cohen, senior vice president of the Information Technology Association of America (ITAA), in Arlington, Va., said there are no "metrics for measuring readiness" against cyber terrorism.

The ITAA has not been able to reach a consensus on whether to support a reporting requirement for cyber security. ITAA President Harris Miller said he personally supports the idea because it would elevate the importance of cyber security to the highest levels within corporations. Miller said he favored a "fairly general" reporting requirement similar to the one put in place in anticipation of possible Y2K computer failures. Those Y2K filings, which reported what companies had done to avert computer crashes when the calendar turned to 2000, varied from one or two sentences to many pages.

Ridge drew a comparison between filing security disclosures with the SEC and the Y2K reporting requirement in an Oct. 9 speech to the Business Software Alliance in Washington, D.C.

Miller said, "My philosophy is if it goes into a [Form] 10-K," an annual earnings report that companies file with the SEC, "it goes to the board of directors."

But some ITAA members fear any sort of filing requirement could lead to a requirement for detailed reports. Their concern is that it could expose vulnerabilities and open companies to potential lawsuits for not having taken certain measures to protect their computer systems.

The possibility of requiring security disclosures in SEC filings is not new. "People are writing white papers and thought

papers" about the idea, said Lewis Stanton, CEO of E Team, a Canoga Park, Calif., crisis management software developer.

It may not be necessary to pass new legislation to require such security filings with the SEC, which has broad authority to require that publicly traded companies disclose all information the commission deems significant to investors.

A 1987 report from the National Commission on Fraudulent Financial Reporting, known as the Treadway Commission after its chairman, former SEC Commissioner James Treadway, also laid the groundwork for requiring companies to report on security, according to Stanton.

"In there, it says that business continuity planning and recovery is an essential element" of a company's operations, Stanton said.

Also, in the Sarbanes-Oxley Act of 2002, passed in the wake of corporate accounting scandals to increase management's accountability, "they do say you've got a responsibility for maintaining an appropriate system of internal controls to ensure business viability," he said.

Find this article at:

http://www.aviationnow.com/avnow/news/channel_hsd_story.jsp?view=story&id=news/req10153.xml



Copyright © 2002 Aviation Week, a division of The McGraw-Hill Companies

All rights reserved. [Terms of Use](#) | [Privacy Policy](#)