Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Recent Trends In Cybersecurity Scrutiny

Law360, New York (October 22, 2012, 2:55 PM ET) -- On the heels of a recent survey that found that cybersecurity is becoming the primary concern of corporate general counsels and directors,[1] the United States government is increasingly taking an active role in addressing cybersecurity issues.

On Sept. 19, 2012, Sen. John D. Rockefeller IV, D-W.Va., — chairman of the U.S. Senate Committee on Commerce, Science and Transportation — sent a letter to the chief executive officers of all Fortune 500 companies addressing the need for better cybersecurity measures and requesting their active involvement in developing such measures.

Sen. Rockefeller stated that "the cyber threats we face are real and immediate, and Congress's failure to pass legislation this year leaves the country increasingly vulnerable to a catastrophic cyber attack." Moreover, Sen. Rockefeller noted that most executives "recognize the gravity of this threat and that their companies would benefit from deeper collaboration with the government."

Sen. Rockefeller's letter comes on the heels of litigation commenced by the Federal Trade Commission against various companies based on their alleged failure to maintain appropriate cybersecurity measures. The letter also follows guidance by the U.S. Securities and Exchange Commission regarding the disclosure requirements for public companies regarding cybersecurity risks and breaches.

On June 12, 2012, the FTC commenced a declaratory judgment proceeding against, among others, Wyndham Worldwide Corporation, seeking injunctive relief against Wyndham for its failure to "maintain reasonable and appropriate data security for consumers' sensitive personal information."

In its complaint, the FTC alleged that Wyndham's "failure to maintain reasonable security allowed intruders to obtain unauthorized access to the computer networks of Wyndham Hotels and Resorts, LLC, and several hotels franchised and managed by Defendants on three separate occasions in less than two years."

This lack of adequate cybersecurity measures led to "fraudulent charges on consumers' accounts, more than $10.6 million in fraud loss, and the export of hundreds of thousands of consumers' payment card account information to a domain registered in Russia."

Moreover, the FTC commenced enforcement actions against two businesses — EPN Inc. and Franklin's Budget Car Sales Inc. — alleging that the businesses illegally exposed "sensitive personal information of thousands of consumers by allowing peer to peer file-sharing software to be installed on their corporate computer systems." Specifically, the businesses' failure to adopt adequate cybersecurity measures subjected personal information, such as social security numbers, to disclosure.

The FTC entered into settlements with both businesses, whereby "both companies must establish and maintain comprehensive information security programs." The settlements also bar "misrepresentations about the privacy, security, confidentiality, and integrity of personal information collected from consumers."

Further, as previously addressed in our article on the availability of insurance coverage for cybersecurity incidents, on Oct. 13, 2011, the SEC issued guidance regarding the disclosure

requirements for public companies arising from cybersecurity risks and breaches.[2] The SEC noted that in disclosing cybersecurity risks, it would be prudent for companies to include a "[d]escription of relevant insurance coverage." See id.

This increased involvement by the federal government further evidences the importance of cybersecurity and protecting against cyber risk through, among other things, adequate insurance coverage. As noted in our recent article, companies may have several avenues to coverage for losses associated with cybersecurity incidents.

Indeed, since we published that article, the Sixth Circuit has issued a pro-policyholder decision regarding coverage for such losses, holding that losses resulting from the theft of customers' banking information are covered under a commercial crime policy's computer fraud endorsement.[3] This ruling further illustrates that the coverage provided by commercial insurance policies can be an extremely valuable corporate asset to companies dealing with cybersecurity issues.

Companies can maximize the benefits of this asset by acting proactively to analyze their insurance portfolio now, and, by being willing to question, and challenge where appropriate, they can maximize coverage denials from their insurers.

--By Barry Buchman, Gilbert LLP

Barry Buchman is a partner in Gilbert's Washington, D.C., office.

The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See C. Dunn, Cybersecurity Becoming No. 1 Concern for GCs and Directors, Corporate Counsel, Aug. 15, 2012.

[2] See Importance Of Procuring Cybersecurity Insurance Coverage, Law360, June 29, 2012.

[3] See Retailer Ventures, Inc. v. Nat'l Union Fire Ins. Co., -- F.3d -- (6th Cir. Aug. 23, 2012).