CATALYST | PARTNERS

May 8, 2015

Via www.sec.gov/cgi-bin/ruling-comments

Mary Jo White

Chair, Offices of the Commissioners

U.S. Securities and Exchange Commission

100 F Street, NE, Room 10700

Washington, DC 20549

Subject: Cybersecurity Roundtable, File No. 4-673.

Dear Chairman White:

I believe that there is a need to address sophisticated threats against American and global enterprises from the perspective of corporate boards and senior executives. Cyber incidents appear to be escalating in frequency, duration, and complexity. I also support the use of effective, relevant, and transparent disclosures to promote efficient capital markets in the area of cyberattacks because without these disclosures, we have "information failure." Investors should be aware of the implications of not disclosing this vital information to all.

Information failure, in economics, can be considered a market failure if some or all of the participants in an economic exchange do not have perfect knowledge. Information failure occurs when one participant in an economic exchange knows more than the other. I refer to this as having asymmetric, or unbalanced, information.

The practical implication is that there is a misallocation of resources meaning that consumers pay too little or too much and firms either produce too little or too much. Information failure is common and appears to exist in numerous market exchanges.

The United States Department of Agriculture addressed this issue as it related to food labeling (http://www.ers.usda.gov/media/532216/aer793.pdf). Their research report on food labeling stated that:

> Government intervention in labeling in the United States has served three main purposes: to ensure fair competition among producers, to increase consumers' access to information, and to reduce risks to individual consumer safety and health.

Some of the same reasoning can be said about buyers and sellers of financial products including stocks and bonds. Disclosing information on cybersecurity ensures fair competition among companies and increases buyers access to information.

Another reason for addressing this issue has to do with something called the principal-agent problem. This can occur when individual decision making relies on the advice of experts who have more knowledge than them. For example, the shareholders of firms, the principals, usually delegate responsibility for day-to-day decision making to appointed managers, the agents. This creates a situation of asymmetric knowledge, with managers knowing much more than the shareholders, and raises the possibility of inefficiencies, especially when shareholders and managers have different objectives. Managers may decide to possibly not reveal certain information to shareholders. They may engage in certain kinds of dealing where they exploit their knowledge of the business's prospects to buy or sell shares and make a personal gain.

There are many other reasons for cybersecurity disclosure rules but the fact that cyber incidents appear to be escalating in frequency, duration, and complexity increases the cost to everyone and the providing of this information creates an environment of more fair competition.

Regards,

Gary S. Becker
Chief Economist, Catalyst Partners,
1250 Connecticut Avenue NW, Suite 825, Washington, DC 20038
[redacted] (Office) [redacted] (Cell)
[redacted]

http://catalystdc.com/about-us/our-team/gary-becker-chief-economist/