There Is No "C" in "ESG": An Illustration of ESG's Biggest Risk

Douglas K. Chia, Soundboard Governance LLC

At its core, ESG stands for the principle that one should identify and consider environmental, social, and governance factors when making business and investment decisions. But this basic concept has morphed into something seriously flawed—elusive to those trying to objectively define it for constructive purposes and at the same time too easily contorted by those with less-than-constructive commercial and political interests.

One of the biggest flaws of ESG is the subjective open-endedness of what counts as E, S, or G. What fits under each is no longer obvious. An example of this is cyber security.

Is Cyber Security ESG?

Corporations manage cyber security along with physical security and other types of business interruption risks. They also examine cyber security in the context of another acronym that starts with E – ERM (enterprise risk management) – typically within the COSO framework.

Now cyber security is also being characterized as an ESG issue. If cyber security is ESG, is it E, S, G, or some combination thereof? Can it be all of them? How far do you have to stretch to make it so? And given cyber security *is* a material risk for most companies, why does this matter?

If forced to assign one letter of ESG to cyber security, the one most proximate is G on the notion that a company's board of directors has a duty oversee cyber security (and ERM more generally) or under the concept of "data governance." But arguments espoused by experts run the gamut. A few are excerpted below.

Cyber is E

Since a corporation's positive environmental policy/impact can potentially benefit those outside its corporate walls, it is considered a public good to contribute to clean air and water. In the same sense, the interconnectedness of today's world means that a corporation's cyber policy, compliance and risk metrics can have far reaching impacts that can cascade throughout society. Organizations with robust cyber security programs—and reporting that gives stakeholders transparency into those programs—are well positioned to improve their ecosystems and safeguard their connections with other associations throughout the world. (KPMG)

The interconnectedness of global economies means that a company's cybersecurity policies, compliance, and risk metrics can have far-reaching impacts on the environment. Companies with robust cybersecurity programs are better positioned…

Leer más