Cyber-Risk Quantification in The Material World

By Vince Dasta

Vince Dasta is director of engagements at VisibleRisk.

A cornerstone of US securities law, according to the Securities Act of 1933, is that public companies have an obligation to publicly disclose information that is significant or material to making informed investment decisions. While materiality has been ingrained in the US Securities and Exchange Commission's (SEC) regulatory approach for almost 90 years, today the term "material" is often overused and even more often under-defined as it pertains to information outside of financial disclosures and accounting misstatements. Recent cyber trends have brought a different type of material event into the limelight.

In 2018, the SEC issued guidance on public company cybersecurity disclosures that emphasizes the importance of "timely disclosures" and of measures to prevent insider trading based on cyber risks or incidents. Although the guidance is a step in the right direction, it lacks clarity on what a material cyber risk is: there are no threshold values for material financial loss, prescriptive quantitative methods, or objective tests to rely on. That said, the SEC indicated that it is reviewing its approach to cyber issues, so we could see further clarification in the coming year.

Driven in part by this (lack of) guidance, the industry has seen an increase in cyber-risk quantification initiatives. To evaluate the materiality of cyber risks, those risks first need to be translated into financial terms. What is missing, however, is a standardized approach to doing so, as the Financial Accounting Standards Board (FASB) has created for accounting. In addition, the industry has focused on quantifying the loss exposure of an organization to certain risks, often neglecting qualitative components of the materiality test that a reasonable investor would consider important.

It is critical to think of cyber-risk quantification as a means to an end and not the end itself. While it may seem counterintuitive, quantitative analysis of cyber risk is only useful in determining materiality when combined with qualitative factors. These include the risk's impact on core products and services and the impact information about the risk might have on the market. They help contextualize the financial loss exposure and meet the accepted tests of materiality.

This is a problem that has been faced before. In fact, in its 1999 bulletin on determining the materiality of accounting misstatements, the SEC wrote, "[The] exclusive reliance on certain quantitative benchmarks to assess materiality in preparing financial statements and performing audits of those financial statements is inappropriate; misstatements are not immaterial simply because they fall beneath a numerical threshold." FASB echoed this in its 2018 Amendments to Financial Accounting Concepts No. 8 in Chapter 3 of the Conceptual Framework for Financial Reporting, "Qualitative Characteristics of Useful Financial Information": "The predominant view is that materiality judgments can properly be made only by those who have all the facts. The Board's present position is that no general standards of materiality could be formulated to take into account all the considerations that enter into an experienced human judgment."

Cyber-risk quantification is a critical component of making a materiality judgment about a particular cyber risk, but the final judgment can only be made by someone with "all the facts." Too often, the results of cyber-risk quantification lack the business context and expert interpretation needed to determine materiality. Tools and statistical analyses may look impressive, but they must be performed and delivered by experts able to contextualize these results within the unique business environment to be useful. Cyber leaders need to understand the business—and speaking in financial terms is only the beginning. D