Cybersecurity

Rethinking Cyber-Risk Maxims

By Jeffrey Batt

Within the ever-expanding cybersecurity ecosystem, certain generalized observations, advice, and one-size-fits-all guidelines for dealing with cyber threats have gained traction as maxims. However, it can be tricky and even dangerous to rely on these guidelines to provide baseline perspectives for understanding the scope of cyber risk, as they tend to oversimplify the issue and increase fear and uncertainty within organizations. Like other corporate risks, cyber risk can be managed through a combination of avoidance, treatment, acceptance, and transfer mechanisms, but its complexity and evolving nature demand a more thorough assessment.

When having conversations about cyber risk, directors and officers should consider the broad implications of any blanket statement offered to them. For example, directors and officers are often told to begin with the following two-step process: first, identify your organization's most valuable data assets to better understand the scope of cyber risk; second, ask what is being done to protect this valuable data in terms of people, process, and technological solutions.

While the first step is undeniably cogent advice, this suggestion is too narrow right off the bat because it focuses only on data. Company leaders would be better served by identifying the following: the organization's core (i.e., most profitable) business operations; how and what these operations produce in terms of goods and services; the organizational business units with operational responsibility for these goods and services; how these business units use, store, and process data; and the extent to which the data is stored and processed in-house versus through outside vendors.

Rather than just identifying valuable data, by the end of this refined process, the organization will likely be able to discover new risks inherent with automation or outsourcing, while also more fully grasping the extent and range of vulnerabilities in its broader supply chain.

Like other corporate risks, cyber risk can be managed through a combination of avoidance, treatment, acceptance, and transfer mechanisms, but its complexity and evolving nature demand a more thorough assessment.

Although the second step initially seems logical in that organizations are commonly encouraged to identify and categorize cyber-risk management solutions with respect to people, processes, and technology, upon closer inspection, few solutions are exclusive to one of these categories. Restricting network access to only certain users is an example of a solution that impacts all three categories: a corporate policy mandates the network access restriction; the restriction is executed by an information security (InfoSec) or information technology (IT) team; and one of the policy's core objectives is to limit human error.

Therefore, it's imperative that organizations think about cybersecurity solutions as interconnected enterprise risk management tools and not in terms of silos. Given the broad and blended nature of these solutions, organizations also need to ensure that the right people are assessing the feasibility of these solutions in terms of cost, time, implementation, and other factors. Ideally, a cross-functional working group or committee comprised of senior officers from finance, InfoSec, IT, legal, privacy, compliance, marketing, and human resources would discuss and make recommendations in connection on a somewhat regular cadence.

As cyber risk continues to evolve, especially in light of emerging issues such as the interconnection of cyber risk and geopolitical risk, increased susceptibility of Internet service providers, ransomware, and an uptick in critical infrastructure targeting, organizations will be well-served to fully explore and flesh out the scope of their cyber-risk exposure. To do so, they must ask the right questions and ensure that their outside partners or advisors—whether lawyers, consultants, brokers, or others—are properly framing the issue as well. Only an in-depth analysis of the complexities of your business operations and risk, along with having the right risk management and transfer tools in place, will increase cyber resiliency.

Jeffrey Batt is a vice president in Marsh's Cyber Practice, where he advises companies on the scope of their cyber risk and related insurance solutions.