SheppardMullin

Articles

What to Do—and What Not to Do—in the Aftermath of a Cybersecurity Attack

Among the most-important: Don't create fear and uncertainty by firing the people who may know best how to recover from the attack

The Wall Street Journal

12.08.2020

Partner Justine Philips discusses how companies should respond to a cybersecurity attack. She emphasizes the importance of developing new policies and recording the breach and how it was resolved to " demonstrate a business has learned and will do better next time." She explains that, "Regulators and consumers want to see that companies took reasonable measures to contain, investigate and remediate the event," and that a record of these changes is essential to "ensure the system is threat-free again, without backdoors."

Attorneys

Justine M. Phillips

Practice Areas

Privacy and Cybersecurity