How Directors Can Mitigate Cyber Risk with the SAFETY Act

This article was originally published by the National Association for Corporate Directors on October 2, 2014.

by Brian E. Finch and Sarah A. Good

Brian E. Finch
Public Policy
+1.202.663.8062
brian.finch@pillsburylaw.com

Brian Finch is a Public Policy partner in Pillsbury's Washington, DC office and is co-leader of the firm's Global Security Services team.

Sarah A. Good
Litigation
+1.415.983.1314
sarah.good@pillsburylaw.com

Sarah Good is a Litigation partner in Pillsbury's San Francisco office. She is a member of the firm's Global Security Services team and is co-leader of the Securities Litigation & Enforcement Team.

There is no shortage of advice on cyber security measures available to corporate directors. What's missing from many discussions about cyber-security however is an exploration of what measures are available to minimize a company's exposure to litigation and financial loss in the aftermath of a cyberattack. This is due in part to the fact that, as of this writing, there is no established cybersecurity baseline directors can point to in order to demonstrate that their actions were reasonable or in line with a standard of care. Fortunately, there's the SAFETY Act, a federal safe harbor law adminis-tered by the Department of Homeland Security that can establish a record of appropriate cybersecurity measures, thereby relieving many concerns associated about whether a company is doing enough to protect itself from cyber threats.

Under the SAFETY Act, a company that sells or deploys cyber security products or services for its own use can, upon demonstrating that the product or service is effective against cyberattacks, potentially receive two types of liability protection:

- **Designation** establishes a maximum limit on civil liability a company can face for the qualified cybersecurity product or service. This limit, which is set through negotiations between the applicant and DHS, is typically equal to a portion of a company's insurance program. Once set, that amount represents an annual aggregate limit of civil liability for any claims arising out of or related to the use of the SAFETY Act protected product/service. Further, a Designation award bars punitive damages and prejudgment interest, and also requires all claims to be litigated in a federal court.
- **Certification** provides the awardee with a rebuttable presumption of immunity from liability. This means that if a company's cybersecurity policies are SAFETY Act Certified, the company can immediately move to dismiss claims alleging that the policies were negligent, defective, or otherwise ineffective. The only way to defeat a Certification is to either show fraud or willful misconduct during the application process, or that the product or service at issue is not covered by the SAFETY Act award.

The protections are obtained by submitting an application for a SAFETY Act award to DHS, and can attach to a wide variety of cyberse-curity policies and products. Most importantly, the SAFETY Act is the only law in existence today that can proactively limit the fallout of lawsuits arising from cyber-attacks.

Beyond helping establish that the security measures taken by the company were reasonable or that due care was exercised, the SAFETY Act also provides an excellent argument against personal liability for directors and officers. Pointing out that the federal government reviewed the company's cybersecurity measures and deemed them effective helps directors demonstrate that they exercised due care in their oversight of the company's cybersecurity program and in mitigating potential litigation in the wake of a cyberattack that could result in a potentially large losses to shareholders..

Here are three key ways directors can ensure the wise use of the SAFETY Act:

- Require that your company audits its internal cybersecurity programs and policies and then submit SAFETY Act applications for cybersecurity items found to be eligible for such protections. By doing so, the company will not only get SAFETY Act liability benefits, it will also have the ability to show that its products and services were meaningfully reviewed by the federal government.
- In security-related contracts, require that the vendor either hold or pursue liability protections under the SAFETY Act. Because the liability protections of the SAFETY Act flow down to a customer, the simple act of buying approved items will also give the company the ability to seek immediate dismissal from claims asserting that the wrong product or service was procured or that it worked improperly.
- Make sure that any future cybersecurity plans, policies, or acquisitions are conducted with the SAFETY Act in mind. By starting from the ground up with the SAFETY Act, directors can more readily be assured that every opportunity possible is being taken to manage liability.

Remember too that the SAFETY Act fits together nicely with cyber insurance. Cyber insurance is important with respect to recovering losses from an attack. However, the global capacity for cyber insurance is very limited—somewhere in the billions of dollars, albeit on the low end—and individual companies can typically obtain no more than $350 million in coverage. Considering that the costs of retail data breaches may exceed $1 billion, that amount seems paltry. So, while companies should buy cyber insurance, they cannot rely on it to fully compensate them, much less set an actual cap on potential losses.

For whatever reason, we seem to have adopted a "blame the cyberattack victim" mentality. Several shareholder suits brought against directors following high-profile cyberattacks confirm that notion—and more litigation will inevitably follow. As these cases are just starting to play out in the courts, it's anyone's best guess as to how the judges will rule.

Directors have to do everything they can then to show that they exercised due care and took all reasonable measures against cyberattacks to preserve shareholder value, and there is no better way to do so than by using the SAFETY Act along with cyber insurance to limit or eliminate liability.